بروتوكول بيركلي

بشأن التحقيقات الرقمية المفتوحة المصدر

دليل عملي بشأن استخدام المعلومات الرقمية المفتوحة المصدر استخداماً فعالاً في التحقيق في انتهاكات القانون الجنائي الدولي والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني

الأمم المتحدة
حقوق الإنسان
مكتب المفوض السامي

HUMAN RIGHTS CENTER
UC Berkeley School of Law

بروتوكول بيركلي

بشأن التحقيقات الرقمية المفتوحة المصدر

دليل عملي بشأن استخدام المعلومات الرقمية المفتوحة المصدر استخداماً فعالاً في التحقيق في انتهاكات القانون الجنائي الدولي والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني

HUMAN RIGHTS CENTER
UC Berkeley School of Law

الأمم المتحدة
حقوق الإنسان
مكتب المفوض السامي

نيويورك وجنيف، 2024

HR/PUB/20/2
ISBN: 978-92-1-154247-9
eISBN: 978-92-1-005346-4
Sales no.: A.20.XIV.4

تشارَك في نشر هذا الدليل الأممُ المتحدة، باسم مفوضية الأمم المتحدة السامية لحقوق الإنسان، ومركزُ حقوق الإنسان في كلية الحقوق في جامعة كاليفورنيا، بيركلي.

ويعرب مركز حقوق الإنسان في كلية الحقوق في جامعة كاليفورنيا، بيركلي، عن امتنانه للدعم المالي الذي تلقاه من الجهات المانحة التالية: Sigrid Rausing Trust؛ وOak Foundation؛ ومن متبرعين أفراد في جامعة كاليفورنيا، بيركلي؛ ومؤسسات المجتمع المفتوح؛ وRockefeller Foundation Bellagio Center.

المحتويات

توطئة

منذ أوائل تسعينات القرن الماضي، أحدثت الأدوات الرقمية والإنترنت، شأنها في ذلك شأن آلات التصوير والهاتف قبلها، ثورة في سبل الحصول على المعلومات عن انتهاكات حقوق الإنسان وغيرها من الانتهاكات الخطيرة للقانون الدولي، بما في ذلك الجرائم الدولية، وفي جمع هذه المعلومات ونشرها.

واليوم، بات بوسع المحققين الحصول على بيانات عن الانتهاكات المحتملة لحقوق الإنسان وغيرها من الانتهاكات الخطيرة للقانون الدولي، ومن بينها الجرائم الدولية، من مجموعة واسعة النطاق من صور الأقمار الصناعية ومقاطع الفيديو والصور المتاحة للجمهور، ومن بينها المواد التي تُحمَّل على الإنترنت من الهواتف الذكية والمنشورات الموضوعة على منصات التواصل الاجتماعي. وأعان هذا التطور المحققين على تجاوز الحكومات وغيرها من القائمين على حراسة بوابات المعلومات التقليديين للنفاذ، حتى في الوقت الفعلي، إلى معلومات رئيسية عن المخالفات كانت، لولا ذلك، ستبقى محجوبة عن الرأي العام.

بيد أنَّ المعلومات الرقمية المفتوحة المصدر استُخدمت إلى حد كبير بشكل غير منتظم لأنَّ منظمات حقوق الإنسان والهيئات الحكومية الدولية وآليات التحقيق والمحاكم واجهت، في بعض الأحيان، صعوبات في تكييف الممارسات التي تتبعها في عملها لتشمل أساليب رقمية جديدة لتقصي الحقائق والتحليل. ومن أصعب التحديات التي تواجهها هذه الجهات كيفية التعامل مع اكتشاف مواد مفيدة والتحقق من صحتها في خضم كم متزايد من المعلومات المنشورة على الإنترنت، وخاصة الصور الفوتوغرافية ومقاطع الفيديو التي تلتقطها الهواتف الذكية وسواها من الأجهزة المحمولة وبعضها قد يشوبه عيب أو يُنسب إلى جهة ما بشكل خاطئ.

وفي الوقت نفسه، أبرز ظهور المحاكم الجنائية وآليات التحقيق الدولية، فضلاً عن الوحدات الوطنية المعنية بجرائم الحرب، الحاجة الماسة إلى معايير مشتركة لالتقاط المعلومات المفتوحة المصدر التي يمكن تقديمها كأدلة في المحاكمات الجنائية وحفظها وتحليلها. وحتى تكون المعلومات المفتوحة المصدر مقبولة كدليل في المحاكم، يجب عادة أن يكون المدعون العامون والمحامون قادرين على إثبات صحتها وسلسلة عُهدتها. ومن شأن التعامل مع هذه المواد وتجهيزها على النحو المناسب أن يزيد احتمال استخدامها من قبل المدعين العامين والمحامين بدرجة كبيرة. أما إن استُخدمت أساليب غير سليمة لجمع المعلومات وحفظها، فسيتعذر عندئذ الاعتداد بموثوقيتها لأغراض إثبات الوقائع في قضية ما. وستعود المعايير الجلية لتقييم وزن المعلومات المفتوحة المصدر، إما باعتبارها أدلة رابطة أو قائمة على الجريمة، بالفائدة على المحاكم وآليات التحقيق. وستكون المعايير المنهجية المشتركة بشأن التوثيق والتحقق كذلك عوناً لبعثات تقصي الحقائق في مجال حقوق الإنسان التي أخذت تضمِّن تحقيقاتها على نحو متزايد مواد رقمية مفتوحة المصدر. ويُتوقع أن تنتفع لجان التحقيق وعناصر حقوق الإنسان في عمليات حفظ السلام والمكاتب الميدانية لمفوضية الأمم المتحدة لحقوق الإنسان وغيرها من جهود الأمم المتحدة لرصد حقوق الإنسان والتحقيق فيها من المبادئ والنهج المنهجية السليمة التي تعزز صحة ما تتوصل إليه هذه الجهات من نتائج وتزيدها ثقلاً.

ولتلبية هذه الحاجة، تضافرت جهود مؤسستينا، أي مركز حقوق الإنسان بكلية الحقوق في جامعة كاليفورنيا ببيركلي ومفوضية الأمم المتحدة السامية لحقوق الإنسان، لنشر *بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة المصدر: دليل عملي بشأن استخدام المعلومات الرقمية المفتوحة المصدر استخداماً فعالاً في التحقيق في انتهاكات القانون الجنائي الدولي والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني*. وبدأ المسار المفضي إلى هذا المنشور في حرم جامعة بيركلي في عام 2009، عندما جمع مركز حقوق الإنسان بين خبراء قانونيين وتقنيين وصحفيين وناشطين لوضع استراتيجيات لاستخدام التقنيات والمنهجيات الرقمية لفضح انتهاكات حقوق الإنسان وتوثيقها. ومنذ ذلك الحين، عقد مركز حقوق الإنسان سلسلة من حلقات العمل المتعددة التخصصات، بالتعاون مع طائفة من الخبراء التقنيين والقانونيين والمعنيين بالمنهجية، بعضهم من المفوضية السامية لحقوق الإنسان، لتبادل الأفكار وإعداد أدوات جديدة وتحديد واستخلاص معايير وأساليب للكشف عن المعلومات الرقمية المفتوحة المصدر وتقييمها والتحقق منها والحفاظ عليها بغية توثيق انتهاكات حقوق الإنسان وتقديم مرتكبيها إلى العدالة. وتتسق هذه العملية أيما اتساق مع الجهود التي تبذلها المفوضية السامية لحقوق الإنسان لوضع ارشادات وأدوات لدعم لجان التحقيق وبعثات تقصي الحقائق التابعة للأمم المتحدة وموظفي المفوضية وإسداء المشورة إليهم في استخدامهم المتزايد للمعلومات المفتوحة المصدر في أعمال تقصي الحقائق والتحقيق.

وساهم في وضع بروتوكول بيركلي أفراد تتنوع منظوراتهم المهنية وخلفياتهم القانونية والثقافية ونوع جنسهم وجنسياتهم. وشمل ذلك إجراء أكثر من 150 مشاورة مع الخبراء ومساهمات من أصحاب المصلحة الرئيسيين، بمن فيهم محققو الأمم المتحدة في مجال حقوق الإنسان. واسترشد البروتوكول أيضاً بخبرة الأفرقة العاملة

المتخصصة في وحدة المنهجية والتعليم والتدريب التابعة لمفوضية حقوق الإنسان ومكتب المدعي العام في المحكمة الجنائية الدولية. ووفقاً للمعايير الدولية لوضع منهجية جديدة، أخضعت المفوضية ومركز حقوق الإنسان بروتوكول بيركلي لعملية صارمة قوامها الاستعراض والتنقيح والتصديق.

وبفضل هذا النهج التعاوني، يتضمَّن بروتوكول بيركلي معايير دولية لإجراء البحوث عبر الإنترنت في الانتهاكات المزعومة للقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني والقانون الجنائي الدولي. ويتيح البروتوكول أيضاً إرشادات بشأن منهجيات وإجراءات جمع المعلومات الرقمية وتحليلها والحفاظ عليها بطريقة مهنية وقانونية وأخلاقية. وختاماً، يحدد بروتوكول بيركلي التدابير التي يمكن للمحققين عبر الإنترنت اتخاذها لحفظ السلامة الرقمية والمادية والنفسية حماية لأنفسهم وللآخرين، ومن بينهم الشهود والضحايا والمستجيبون الأوائل (مثل المواطنين والناشطين والصحفيين)، الذين يخاطرون بسلامتهم لتوثيق انتهاكات حقوق الإنسان والانتهاكات الخطيرة للقانون الدولي.

ويسير بروتوكول بيركلي على خطى بروتوكولين سابقين للأمم المتحدة هما: بروتوكول مينيسوتا المتعلق بالتحقيق في حالات الوفاة التي يُحتمل أن تكون غير مشروعة (1991، تم تحديثه في عام 2016) ودليل التقصي والتوثيق الفعالين للتعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة (بروتوكول اسطنبول) (1999، تم تحديثه في عام 2004). ويضع بروتوكول مينيسوتا الذي أعدَّه محامون وعلماء في الأدلة الجنائية يشاركون في البحث عن الأشخاص المختفين في الثمانينات معايير وإجراءات دولية لإجراء التحقيقات الطبية والقانونية في الوفيات المشبوهة أو غير المعايَنة، وهو يُستخدم وسيلة لتقييم مصداقية هذه التحقيقات. وبالمثل، يقدم بروتوكول اسطنبول إرشادات للممارسين الطبيين والمحامين عن سبل التعرف على آثار التعذيب المادية الجسدية والنفسية وتوثيقها على نحو يجعل الوثائق أدلة صالحة في المحاكم أو في سياقات أخرى، بما في ذلك التحقيقات والرصد في مجال حقوق الإنسان. وتستند البروتوكولات الثلاثة جميعها إلى الاعتقاد بأنَّ بوسع العلم والتكنولوجيا والقانون – بل ويجب عليها – أن تعمل معاً في خدمة حقوق الإنسان. وعلى غرار البروتوكولات السابقة، سيتاح بروتوكول بيركلي باللغات الرسمية للأمم المتحدة، تيسيراً لاستخدامه وتعميماً لفائدته في كل أنحاء العالم.

ويحدونا الأمل في أن يساعد بروتوكول بيركلي، في عالم ما برح يزداد رقمنة، المحققين عبر الإنترنت – سواء أكانوا مهنيين قانونيين أو مدافعين عن حقوق الإنسان أو صحفيين أو غيرهم – على وضع وتنفيذ إجراءات فعالة ومتحقق منها لتوثيق انتهاكات القانون الدولي لحقوق الإنسان، والقانون الدولي الإنساني، والقانون الجنائي الدولي، من خلال الاستفادة القصوى من المعلومات الرقمية المفتوحة المصدر، حتى يتسنى تقديم المسؤولين عن هذه الانتهاكات إلى العدالة بشكل منصف.

إريك ستوفر
مدير هيئة التدريس، مركز حقوق الإنسان،
جامعة كاليفورنيا، بيركلي، كلية الحقوق

ميشيل باشليت
مفوضة الأمم المتحدة السامية
لحقوق الإنسان

موجز تنفيذي

التحقيقات المفتوحة المصدر هي تحقيقات تعتمد، اعتماداً كلياً أو جزئياً، على المعلومات المتاحة للجمهور لإجراء تحقيقات رسمية ومنهجية عبر الإنترنت في المخالفات المزعومة. واليوم، يمكن الحصول على كم هائل من المعلومات المتاحة للجمهور من خلال شبكة الإنترنت، حيث أحدث المشهد الرقمي السريع التطور أنواعاً ومصادر جديدة من المعلومات يمكن أن يُستعان بها في التحقيق في انتهاكات حقوق الإنسان المزعومة وفي الجرائم الدولية الخطيرة. وتكتسي القدرة على التحقيق في هذه الادعاءات أهمية خاصة لدى المحققين الذين يتعذر عليهم الوصول بأنفسهم إلى مسارح الجرائم في الوقت المناسب، وهو أمر يحدث في التحقيقات الدولية في كثير من الأحيان.

ويمكن للمعلومات المفتوحة المصدر أن تتيح أدلة وتدعم معلومات الاستخبارات وتشكل دليلاً مباشراً في المحاكم. بيد أنَّ استخدام هذه المعلومات في عمليات التحقيق الرسمية، بما في ذلك التحقيقات القانونية وبعثات تقصي الحقائق ولجان التحقيق، يقتضي أن يتّبع المحققون أساليب متسقة تعزز دقة استنتاجاتهم وتمكِّن القضاة وغيرهم من المتقصين للحقائق من تقييم نوعية عملية التحقيق نفسها تقييماً أفضل. وأُعِدَّ بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة المصدر لإتاحة معايير وارشادات دولية للمحققين في مجالات العدالة الجنائية الدولية وحقوق الإنسان. وينتمي هؤلاء المحققون إلى طائفة من المؤسسات، من بينها وسائل الإعلام ومجموعات المجتمع المدني والمنظمات غير الحكومية والمنظمات الدولية والمحاكم ووكالات التحقيق الوطنية والدولية. ويشكِّل إنشاء معايير متسقة وقابلة للقياس تدعم هذا المجال المتعدد التخصصات وسيلة لإضفاء الطابع المهني على ممارسة التحقيقات المفتوحة المصدر.

ولئن كانت المبادئ التوجيهية والتدريب على استخدام أدوات وبرامج محددة جزءاً أساسياً لتجويد التحقيقات الرقمية المفتوحة المصدر، فإنَّ بروتوكول بيركلي لا يركز على تكنولوجيات أو منصات أو برمجيات أو أدوات محددة، بل على المبادئ والمنهجيات الأساسية التي يمكن تطبيقها باستمرار، حتى وإن تغيرت التكنولوجيا نفسها. وتحدد هذه المبادئ الحد الأدنى من المعايير القانونية والأخلاقية لإجراء تحقيقات فعالة مفتوحة المصدر. وباتباع الإرشادات الواردة في بروتوكول بيركلي، سيزيد المحققون عملهم جودةً، مقللين في الوقت ذاته الأخطار المادية الجسدية والنفسية الاجتماعية والرقمية التي قد يتعرضون لها هم وسواهم.

وأُعِدَّ بروتوكول بيركلي ليكون أداة تعليمية ودليلاً مرجعياً للمحققين المتخصصين في المصادر المفتوحة. وتُكرَّس الفصول الثلاثة التي تلي الفصل الاستهلالي للأطر الشاملة، ومن بينها المبادئ والاعتبارات القانونية والأمن. ويُركَّز في باقي الفصول على عملية التحقيق نفسها. ويبدأ هذا الفرع من بروتوكول بيركلي بفصل يتناول الإعداد والتخطيط الاستراتيجي، يليه فصل مخصص لمختلف خطوات التحقيق المطلوبة – وهي عمليات الاستقصاء عبر الإنترنت والتقييم الأولي وجمع المعلومات وحفظها والتحقق من صحتها والتحليل الاستقصائي. ويُختتم الفرع بفصل عن منهجية ومبادئ الإبلاغ عن نتائج التحقيق المفتوح المصدر.

المساهمون والمشاركون

لجنة تنسيق بروتوكول بيركلي

ليندسي فريمان، باحثة قانونية أولى، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

أليكسا كونيغ، المديرة التنفيذية، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

إريك ستوفر، مدير هيئة التدريس، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

لجنة تحرير بروتوكول بيركلي

ساريتا أشرف، مستشارة قانونية أولى؛ محامية، دوائر محكمة غاردن كورت؛ محللة أولى سابقة، فريق التحقيق التابع للأمم المتحدة لتعزيز المساءلة عن الجرائم المرتكبة من جانب داعش/تنظيم الدولة الإسلامية في العراق والشام.

أليكس دن، المدير التنفيذي، The Engine Room

ريتشارد غولدستون، قاض سابق، المحكمة الدستورية لجنوب أفريقيا؛ كبير المدعين العامين السابق، المحكمة الدولية الجنائية ليوغوسلافيا السابقة، والمحكمة الجنائية الدولية لرواندا

بريندا ج. هوليس، المدعية العامة الدولية المعاونة، الدوائر الاستئنافية في محاكم كمبوديا؛ كبيرة المدعين العامين السابقة، محكمة سيراليون الخاصة لتصريف الأعمال المتبقية

تانيا كاراناسيوس، مديرة البرامج في منظمة WITNESS

إنريكي بيراسيس، مدير برنامج الإعلام وحقوق الإنسان، مركز علوم حقوق الإنسان، جامعة كارنيغي ميلون

بيث فان شاك، أستاذة زائرة في مجال حقوق الإنسان، كلية الحقوق بجامعة ستانفورد؛ النائبة السابقة للسفير المتجول المعني بقضايا جرائم الحرب، مكتب العدالة الجنائية العالمية، وزارة خارجية الولايات المتحدة

ميشيل دي سميدت، مدير شعبة التحقيقات، مكتب المدعي العام، المحكمة الجنائية الدولية

آلان تيغر، وكيل أول للمدعي العام، مكتب المدعي العام المتخصص لكوسوفو؛ وكيل أول سابق للمدعي العام، المحكمة الدولية ليوغوسلافيا السابقة

كريستيان فينافيسر، الممثل الدائم لليختنشتاين لدى الأمم المتحدة؛ الرئيس السابق لجمعية الدول الأطراف في نظام روما الأساسي للمحكمة الجنائية الدولية

أليكس وايتنغ، رئيس التحقيقات، مكتب المدعي العام المتخصص لكوسوفو؛ أستاذ الممارسة، كلية الحقوق بجامعة هارفارد؛ منسق الادعاء العام ومنسق التحقيقات السابق، مكتب المدعي العام، المحكمة الجنائية الدولية

سوزان وولفنبارغر، مسؤولة الشؤون الخارجية ورئيسة فريق التحليلات، وزارة خارجية الولايات المتحدة؛ مديرة مشروع أولى سابقة، مشروع التكنولوجيات الجغرافية المكانية، الرابطة الأمريكية لتقدم العلم

اللجنة الاستشارية لبروتوكول بيركلي

فيديريكا داليساندرا، المديرة التنفيذية، برنامج أكسفورد للسلم والأمن الدوليين، جامعة أكسفورد؛ محررة *دليل الفريق المعني بالقانون الدولي العام والسياسات بشأن توثيق المجتمع المدني للانتهاكات الخطيرة لحقوق الإنسان: المبادئ والممارسات الفضلى*

ستيوارت كيسي – ماسلين، أستاذ فخري، كلية الحقوق، جامعة بريتوريا؛ مساهم في *بروتوكول مينيسوتا المتعلق بالتحقيق في حالات الوفاة التي يُحتمل أن تكون غير مشروعة (2016)*

أليسون كول، مستشارة متخصصة في حقوق الإنسان، إدارة الشؤون الداخلية، نيوزيلندا

فرانسواز هامبسون، أستاذة فخرية، كلية الحقوق بجامعة إسكس؛ عضوة لجنة التحقيق بشأن بوروندي

كريستوف هاينز، أستاذ قانون حقوق الإنسان، جامعة بريتوريا؛ عضو في اللجنة المعنية بحقوق الإنسان؛ المقرر الخاص السابق المعني بحالات الإعدام خارج القضاء أو بإجراءات موجزة أو تعسفاً؛ منسق *بروتوكول مينيسوتا المتعلق بالتحقيق في حالات الوفاة التي يُحتمل أن تكون غير مشروعة (2016)*

فنسنت إياكوبينو، مستشار طبي أول، أطباء من أجل حقوق الإنسان؛ مساهم رئيسي في *دليل التقصي والتوثيق الفعالين للتعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة (بروتوكول اسطنبول)*

كيلي ماثيسون، محامية أولى ومديرة برنامج في منظمة WITNESS؛ مؤلفة *الدليل الميداني للفيديو كدليل*

هاني مجلي، مفوض، لجنة التحقيق الدولية المستقلة المعنية بالجمهورية العربية السورية؛ زميل أقدم، مركز التعاون الدولي، جامعة نيويورك

خوان منديز، أستاذ قانون حقوق الإنسان المقيم، كلية واشنطن للقانون؛ المقرر الخاص السابق المعني بمسألة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة؛ منسق البروتوكول العالمي لإجراء المقابلات الاستقصائية والضمانات الإجرائية

أريبه نير، الرئيس الفخري، مؤسسات المجتمع المفتوح

نافي بيلاي، رئيسة اللجنة الدولية لمناهضة عقوبة الإعـدام؛ مفوضة الأمم المتحدة السامية السابقة لحقوق الإنسان؛ قاضية سابقة، المحكمة الجنائية الدولية؛ الرئيسة السابقة للمحكمة الجنائية الدولية لرواندا

باولو سيرجيو بينهيرو، رئيس لجنة التحقيق الدولية المستقلة المعنية بالجمهورية العربية السورية؛ المقرر الخاص السابق المعني بحالة حقوق الإنسان في بوروندي؛ المقرر الخاص السابق المعني بحالة حقوق الإنسان في ميانمار

توماس بروبرت، محاضر فوق العادة، مركز حقوق الإنسان، جامعة بريتوريا؛ باحث مشارك، مركز الحوكمة وحقوق الإنسان، جامعة كيمبريدج؛ مساهم في *بروتوكول مينيسوتا المتعلق بالتحقيق في حالات الوفاة التي يُحتمل أن تكون غير مشروعة (2016)*

ستيفن راب، زميل متميز، مركز سيمون – سكجودت لمنع الإبادة الجماعية، متحف الولايات المتحدة التذكاري للهولوكوست؛ سفير متجول سابق لقضايا جرائم الحرب، مكتب العدالة الجنائية العالمية، وزارة خارجية الولايات المتحدة؛ المدعي العام السابق، المحكمة الخاصة لسيراليون

كريستينا رييبرو، منسقة التحقيقات، مكتب المدعي العام، المحكمة الجنائية الدولية

باتريشيا سيلرز، المستشارة الخاصة المعنية بالمسائل الجنسانية لدى المدعي العام للمحكمة الجنائية الدولية؛ زميلة زائرة، كلية كيلوغ، جامعة أكسفورد؛ مستشارة قانونية سابقة ومحامية ادعاء، المحكمة الدولية ليوغوسلافيا السابقة والمحكمة الجنائية الدولية لرواندا

المشاركون في حلقات العمل

حلقة عمل حول علم الأدلة الجنائية الجديد: استخدام المعلومات المفتوحة المصدر للتحقيق في الجرائم الخطيرة (بيلاجيو، إيطاليا، 2017)

هادي الخطيب، الأرشيف السوري

ستيوارت كيسي ماسلين، جامعة بريتوريا

يفان كوبيرز، المحكمة الجنائية الدولية

سكوت إدواردز، منظمة العفو الدولية

ليندسي فريمان، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

أليكسا كونيغ، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

ستيف كوستاس، مبادرة العدالة في المجتمع المفتوح

أندريا لامبروس، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

كيلي ماثيسون، منظمة WITNESS

فيليم مكماهون، المحكمة الجنائية الدولية

جوليان نيكولز، المحكمة الجنائية الدولية

توماس بروبرت، جامعة كامبريدج

كريستينا رييبرو، المحكمة الجنائية الدولية

غافين شيريدان، Vizlegal

إريك ستوفر، مركز حقوق الإنسان جامعة كاليفورنيا، بيركلي، كلية الحقوق

آلان تيغر، المحكمة الدولية الجنائية ليوغوسلافيا السابقة

مارك واتسون، لجنة العدالة والمساءلة الدولية

غاي ويلوبي، رابطة دراسة جرائم الحرب

حلقة عمل حول إنشاء إطار أخلاقي للتحقيقات المفتوحة المصدر (جامعة إسكس، المملكة المتحدة، 2019)

فْرد أبراهامز، منظمة هيومن رايتس ووتش

لينا بسوني، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

فيديريكا داليساندرا، جامعة أكسفورد

سام دوبرلي، منظمة العفو الدولية

جنيفر إيستردايي، JustPeace Labs

سكوت إدواردز، منظمة العفو الدولية

ليندساي فريمان، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

جيف جيلبرت، جامعة إسكس

كريستوفر"كيب" هيل، لجنة العدالة والمساءلة الدولية

إيفانا هو، Omelas

غابرييلا إيفنز، زميلة في Mozilla ومنظمة WITNESS

أليكسا كونيغ، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

مات محمودي، جامعة كمبريدج

لورنا ماكغريغور، جامعة إسكس

داراغ موراي، جامعة إسكس

فيفيان نغ، جامعة إسكس

إنريكي بيراسيس، مركز علوم حقوق الإنسان، جامعة كارنيجي ميلون

زارا رحمن، The Engine Room

ساشا روبحمد، The Engine Room

إيليا سياتيتسا، المنظمة الدولية لحماية الخصوصية

ممثل المفوضية السامية لحقوق الإنسان، من قسم المنهجيات والتعليم والتدريب*

اجتماع المائدة المستديرة حول القضايا القانونية الناشئة عن تحقيقات المصادر المفتوحة (لاهاي، 2019)

ديفيد أكيرسون، فريق التحقيق التابع للأمم المتحدة لتعزيز المساءلة عن الجرائم المرتكبة من جانب داعش/تنظيم الدولة الإسلامية في العراق والشام

ساريتا أشرف، Garden Court Chambers

دانيا تشايكيل، مكتب الادعاء العام المتخصص لكوسوفو

آلان كلارك، المحكمة الجنائية الدولية

فيديريكا داليساندرا، جامعة أكسفورد

نيكو ديكنز، Bellingeat

كريس إنجلز، لجنة العدالة والمساءلة الدولية

ليندسي فريمان، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

إيما إيرفينغ، جامعة لايدن

ميشيل جارفيس، الآلية الدولية المحايدة المستقلة للمساعدة في التحقيق والملاحقة القضائية للأشخاص المسؤولين عن الجرائم الأشد خطورة وفق تصنيف القانون الدولي المرتكبة في الجمهورية العربية السورية منذ آذار/مارس 2011

إدوارد جيريمي، المحكمة الجنائية الدولية

آشلي جوردانا، منظمة الامتثال العالمي للحقوق

سانغ مين كيم، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

أليكسا كونيغ، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

نيكولاس كومجيان، آلية التحقيق المستقلة لميانمار

باستيان فان دير لاكن، الآلية الدولية المحايدة المستقلة للمساعدة في التحقيق والملاحقة القضائية للأشخاص المسؤولين عن الجرائم الأشد خطورة وفق تصنيف القانون الدولي المرتكبة في الجمهورية العربية السورية منذ آذار/مارس 2011

ديربلا مينوغ، الشبكة العالمية للعمل القانوني

نيك أورتيز، جامعة لايدن

ماتيفز بيزديرك، شبكة الإبادة الجماعية التابعة لوكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية،

سانيا بوبوفيتش، مكتب الادعاء المتخصص لكوسوفو

ستيفن باولز، Doughty Street Chambers؛ لجنة جرائم الحرب التابعة لرابطة المحامين الدولية

ستيفن راب، مركز سيمون سكجودت لمنع الإبادة الجماعية، متحف الولايات المتحدة التذكاري للهولوكوست

كريستينا ريبيرو، المحكمة الجنائية الدولية

مارك روبسون، لجنة العدالة والمساءلة الدولية

براد صموئيلز، SITU Research

دليلة سيوان، Civitas Maxima

كارستن ستان، جامعة لايدن

ميليندا تايلور، المحكمة الجنائية الدولية

آلان تيغر، مكتب الادعاء المتخصص لكوسوفو

راكيل فازكيز ليورنتي، مؤسسة eyeWitness to Atrocities

مراجعون خبراء إضافيون

إليز بيكر، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

شون بروكس، مركز الأمـن السيبراني طويل الأجـل، جامعة كاليفورنيا، بيركلي

ستيفاني كروفت، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

سام دوبرلي، منظمة العفو الدولية

توماس إدوين، مركز الدراسات المتقدمة في شؤون الدفاع

كريستوفر "كيب" هيل، لجنة العدالة والمساءلة الدولية

غابرييلا إيفنز، هيومن رايتس ووتش

فيليم مكماهون، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

داراغ موراي، جامعة إسكس

إيفون نغ، منظمة WITNESS

زارا رحمن، The Engine Room

مارك روبسون، لجنة العدالة والمساءلة الدولية

جاستن سيتز، Hunchly

أندريا تريوينارد، مركز حقوق الإنسان، جامعة كاليفورنيا، بيركلي، كلية الحقوق

ستيف تروش، مركز الأمن السيبراني الطويل الأجل، جامعة كاليفورنيا، بيركلي

راكيل فازكيز يورنتي، مؤسسة eyeWitness to Atrocities

شكر وتقدير خاصين

نخص بالشكر أعضاء الفريق العامل المعني بالتحقيقات عبر الإنترنت، مكتب المدعي العام، المحكمة الجنائية الدولية.

ونشيد أيضاً بدور العديد من الزملاء من المفوضية السامية لحقوق الإنسان الذين أسفرت جهودهم عن إنجاز هذا المنشور المشترك*.

* تقتضي سياسة المفوضية السامية لحقوق الإنسان ألا تُنسب المساهمات في منشوراتها إلى موظفيها.

أولاً

مقدمة

موجز الفصل

- الغرض
- الجمهور المستهدف
- التعاريف

1- يبيِّن بروتوكول بيركلي بشأن التحقيقات الرقمية المفتوحة المصدر المعايير المهنية التي ينبغي تطبيقها في تحديد المعلومات الرقمية المفتوحة المصدر وجمعها وحفظها وتحليلها وعرضها واستخدامها في التحقيقات الجنائية وتحقيقات حقوق الإنسان الدولية. والمعلومات المفتوحة المصدر هي معلومات يمكن لأي فرد من الجمهور ملاحظتها أو ابتياعها أو طلبها دون حاجة إلى وضع قانوني خاص أو اللجوء إلى نفاذ غير مأذون به. والمعلومات الرقمية المفتوحة المصدر هي معلومات متاحة للجمهور في شكل رقمي يتحصل عليها بوجه عام من الإنترنت. وتشمل المعلومات الرقمية المفتوحة المصدر كلاً من البيانات التي ينشئها المستخدمون والبيانات التي تستحدثها الآلات وقد تشمل، على سبيل المثال: المحتوى المنشور على وسائل التواصل الاجتماعي والوثائق والصور ومقاطع الفيديو والتسجيلات الصوتية الموضوعة على المواقع الشبكية ومنصات تبادل المعلومات والصور المرسلة من السواتل والبيانات المنشورة من قبل الحكومات[1]. أما التحقيقات الرقمية المفتوحة المصدر فهي تحقيقات تستند إلى معلومات رقمية مفتوحة المصدر. وتيسيراً للقراءة، سيشير البروتوكول في ما يلي إلى المعلومات والتحقيقات الرقمية المفتوحة المصدر باسم "المعلومات المفتوحة المصدر" و"التحقيقات المفتوحة المصدر"، على التوالي.

2- ومع أنَّ استخدام المعلومات المفتوحة المصدر في التحقيقات ليس بالأمر الجديد، فإنَّ المصادر المفتوحة قد أضحت أوسع نطاقاً وأكثر تنوعاً نتيجة للاستخدام المتزايد للإنترنت وغيره من الموارد الرقمية لتقاسم المعلومات، ويشمل ذلك انتشار وسائل التواصل الاجتماعي. ويتناول هذا البروتوكول كلاً من التعقيدات التي تنشأ عند التعامل مع المعلومات الرقمية والتحديات الفريدة المقترنة بتقييم المصادر والتحقق من صحة المعلومات الموجودة في المنتديات المفتوحة على الإنترنت.

3- ولئن كان عدد ما برح يزداد من المحققين الدوليين في مجال الجرائم الجنائية وحقوق الإنسان يستخدمون الآن الإنترنت لتيسير عملهم، فلا توجد في الوقت الحالي مراجع أو مبادئ توجيهية أو معايير عالمية للتحقيقات المفتوحة المصدر. ويسعى هذا البروتوكول إلى سد هذه الفجوة بوضع مبادئ وممارسات من شأنها أن تعين المحققين على أداء عملهم وفقاً لمعايير مهنية وأن تيسر، عند الاقتضاء، حفظ المعلومات المفتوحة المصدر لاستخدامها المحتمل من قبل آليات المساءلة.

4- ويركز البروتوكول بوجه خاص على التحقيقات المفتوحة المصدر التي تُجرى لأغراض ضمان العدالة والمساءلة على الصعيد الدولي، وهي تشمل بوجه عام: توثيق حقوق الإنسان وحفظها وجمع الأدلة وتقصي الحقائق والتحقيقات التي تجريها لجان التحقيق وبعثات تقصي الحقائق[2]؛ وأنواعاً أخرى من التحقيقات والتحريات المخولة دولياً[3]؛ وعمليات البحث عن الحقيقة والمصالحة والتقاضي المدني والمحاكمات الجنائية، بما في ذلك الإجراءات الجنائية الدولية. وبما أنَّ التحقيقات المفتوحة المصدر يمكن أن تسهم في أنواع مختلفة من الجهود المبذولة لضمان المساءلة[4]، فقد تكون متطلبات المنهجية والتوثيق المبيَّنة في البروتوكول أكثر صرامة من نظيرتها المستخدمة عادة في مجالات أخرى، مثل الصحافة ومناصرة حقوق الإنسان. وأياً كان الغرض المنشود من التحقيق الذي يجريه المحققون المتخصصون في المصادر المفتوحة، فإنَّ التزامهم بالمبادئ المنهجية المبيَّنة في هذا البروتوكول المصممة وفقاً للمعايير

(1) هذه القائمة ليست شاملة. 62

(2) لجان التحقيق وبعثات تقصي الحقائق هي هيئات يمكن أن تنشئها الحكومات أو المنظمات الدولية للتحقيق في مسائل مختلفة. وتقدم لجان التحقيق أو بعثات تقصي الحقائق تقارير عن نتائج الوقائع وتستخلص استنتاجات قانونية وتقدم توصيات. ومع أنَّ النتائج التي تتوصل إليها لجان التحقيق أو بعثات تقصي الحقائق الدولية ليست ملزمة قانوناً، فإن تأثيرها قد يكون شديداً. بيد أنَّ استنتاجات لجان التحقيق الوطنية قد تكون ملزمة في بعض الولايات القضائية. وللاطلاع على مزيد من المعلومات عن لجان التحقيق وبعثات تقصي الحقائق الدولية، انظر مجلس حقوق الإنسان، "لجان التحقيق الدولية ولجان حقوق الإنسان وبعثات تقصي الحقائق، وغيرها من التحقيقات". يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/ar/hr-bodies/hrc/co-is.

(3) انظر، على سبيل المثال، تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان عن حالة حقوق الإنسان في جمهورية فنزويلا البوليفارية (A/HRC/41/18)، المقدم عملاً بقرار مجلس حقوق الإنسان 1/39. انظر أيضاً قرار المجلس 2/41 الذي طلب فيه المجلس إلى المفوضة السامية أن تعد تقريراً عن حالة حقوق الإنسان في الفلبين.

(4) على سبيل المثال، استخدمت البعثة الدولية المستقلة لتقصي الحقائق في ميانمار معلومات مفتوحة المصدر، إلى جانب مصادر مباشرة ومعلومات أخرى، في عملية التحقق التي أجرتها وفي نتائجها واستنتاجاتها. وكان التقرير النهائي لبعثة تقصي الحقائق (A/HRC/42/50) أحد العوامل التي حدت بمجلس حقوق الإنسان إلى إنشاء آلية التحقيق المستقلة لميانمار التي أسندت إليها ولاية إجراء تحقيقات قضائية. وكُلِّفت بعثة تقصي الحقائق أيضاً بتسليم معلوماتها، بما في ذلك محتوى تحقيقاتها المفتوحة المصدر، إلى آلية التحقيق المستقلة لميانمار. واعتمدت غامبيا أيضاً على تقارير بعثة تقصي الحقائق في القضية التي رفعتها ضد ميانمار أمام محكمة العدل الدولية بسبب انتهاك ميانمار لاتفاقية منع جريمة الإبادة الجماعية والمعاقبة عليها. ويبيِّن ذلك كيف يمكن أن تسهم المعلومات التي تُجمع لغرض ما في نهاية المطاف في عملية مساءلة قانونية أخرى.

القانونية المشتركة سيضمن أن تكون أعمالهم عالية الجودة وسيزيد إلى أقصى حد الاستخدام المحتمل للمعلومات المجمعة في المحاكم والهيئات القضائية وفي غيرها من العمليات لضمان المساءلة.

5- وبالإضافة إلى ذلك، يشدِّد البروتوكول على معايير التحقيق في انتهاكات القانون الدولي، ومن بينها انتهاكات حقوق الإنسان وانتهاكات القانون الجنائي الدولي التي تشمل جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية. وفضلاً عن ذلك، يمكن تطبيق التوجيهات التي يتيحها البروتوكول على أنواع أخرى من التحقيقات مثل التحقيقات المتعلقة بالمحاكم الوطنية أو البلدية.

6- وتكمن الغاية المنشودة من وراء إعداد هذا البروتوكول في مساعدة المحققين المتخصصين في المصادر المفتوحة على أداء عملهم وفقاً لمنهجية مهنية تتسق إلى حد كبير مع المتطلبات القانونية والمعايير الأخلاقية. ويهدف البروتوكول أيضاً إلى مساعدة مختلف المستخدمين النهائيين لعملية التحقيق، بمن فيهم المحامون والقضاة وغيرهم من متخذي القرارات، على فهم تقنيات التحقيق المفتوحة المصدر وتقييمها بشكل أفضل. ويرمي البروتوكول أيضاً إلى أن يكون معيناً للممارسين ذوي الخبرة وأداة تدريب وتعليم لمن يرغبون في أن يتعلموا سبل إجراء تحقيقات مفتوحة المصدر في انتهاكات القانون الدولي المزعومة[5].

ألف- الغرض

7- ظلَّ المحققون يعتمدون منذ فترة طويلة على المعلومات المفتوحة المصدر، غير أنَّ وتيرة استغلال هذه المعلومات بانتظام تسارعت في الفترة الممتدة من مطلع القرن العشرين إلى منتصفه مع التركيز على استخراج المعلومات الاستخبارية من البث الإذاعي الأجنبي والصحف المطبوعة[6]. ومع استحداث الشبكة العالمية في التسعينات وما تلاها من انتشار وسائل الإعلام الاجتماعية والهواتف الذكية في الألفية الثانية، تغيرت المعلومات المفتوحة المصدر كماً ونوعاً بشكل عميق. واليوم، بوسع أي شخص بحوزته هاتف ذكي ويستطيع استخدام الإنترنت إنشاء محتوى رقمي وتوزيعه في شتى أنحاء العالم، وإن تفاوتت درجة جودته وصحته وشفافيته. وأتاح تزايد حجم البيانات وسرعة تناقلها وتبادلها فرصاً جديدة للمحققين المتخصصين في المصادر المفتوحة لجمع المعلومات المتعلقة بالجرائم الدولية وانتهاكات حقوق الإنسان وتحليلها. وفي الوقت نفسه، يستطيع منشئو المحتوى الآن نشر المعلومات المضلِّلة والتلاعب بالبيانات الرقمية بسهولة نسبية. ويمثِّل هذا البروتوكول محاولة للتجاوب مع هذه البيئة الجديدة ومع التعقيد الذي يتسم به التعامل مع هذه الفرص والتحديات.

8- وللمعلومات المفتوحة المصدر فائدة في جميع أنواع التحقيقات، وإن كانت تقوم بدور حاسم بوجه خاص في التحقيقات الجنائية الدولية وتحقيقات حقوق الإنسان. ويعود هذا الأمر إلى أسباب عديدة. أولاً، تتوقف التحقيقات المأذون بإجرائها دولياً، ومن بينها التحقيقات التي تجريها لجان التحقيق وبعثات تقصي الحقائق التابعة للأمم المتحدة أو تلك التي تأذن بها المحكمة الجنائية الدولية، على العمليات القانونية والسياسية التي تسمح بإجراء التحقيق. ولذلك، فهي تُجرى، في أحيان كثيرة، بعد وقوع الأحداث بوقت طويل[7]. ثانياً، قد لا تتمكن التحقيقات الدولية، في أحيان كثيرة، من الوصول إلى الموقع المادي الذي وقعت فيه الأحداث قيد التحقيق، على سبيل المثال، بسبب رفض دولة التعاون أو السماح بالنفاذ إلى الموقع. ثالثاً، حتى وإن سُمح للمحققين بالنفاذ إلى منطقة أو إقليم، فقد يكون وصولهم بأنفسهم إلى الموقع المعني محدوداً، أو قد تقام أمامهم عوائق تعرقل إجراء التحقيقات في الموقع أو المقابلات الشخصية بسبب مخاوف تتعلق بالحماية. وخلاصة القول إنَّ معظم المحققين لن يتمتعوا بسلطات إنفاذ القانون الكاملة على الأراضي التي وقعت فيها الجرائم أو الانتهاكات المزعومة. ومن ثم، فهم قد يعجزون عن جمع المعلومات اللازمة. وحتى في الحالات التي تتعاون فيها الدول، قد يكون جمع الأدلة عبر الحدود عملية شاقة وبطيئة بسبب الإجراءات البيروقراطية المعيقة. وتوضح كل هذه العوامل السبب الذي يُكسب تقنيات التحقيق المفتوحة المصدر التي يمكن إجراؤها عن بعد وبشكل متزامن مع وقوع الأحداث قوة ويجعلها ضرورية.

9- ويستهدف البروتوكول مجموعة متنوعة من المحققين العاملين في سياقات مختلفة ووفق ولايات وسلطات وموارد تحقيق متباينة. ولذلك، فهو يتبع نهجاً مرناً لا يتوقع أن يقوم المحققون بعملهم بشكل متطابق، بل يكيفون بالأحرى المنهجيات حسبما

(5) يقدم البروتوكول أيضاً بعض نماذج التحقيقات المفتوحة المصدر، فضلاً عن مسرد مصطلحات (انظر الفصل الثامن أدناه).

(6) Nikita Mehandru and Alexa Koenig, "ICTs, social media, & the future of human rights", Duke Law & Technology Review, vol. 17, No. 1, p. 129.

(7) أنشأ مجلس الأمن والجمعية العامة ومجلس حقوق الإنسان والأمين العام، وجهات أخرى، لجان للتحقيق وبعثات لتقصي الحقائق. وفي حالة المحكمة الجنائية الدولية، يمكن لمكتب المدعي العام أن يبدأ تحقيقات بناء على إحالات من الدول الأطراف أو من مجلس الأمن، أو بمبادرة منه وبإذن من القضاة.

تقتضيه كل بيئة عمل بعينها. وعلاوة على ذلك، وبما أنَّ التكنولوجيات والأدوات والتقنيات التي تساعد التحقيقات المفتوحة المصدر تتطور باستمرار، فإنَّ البروتوكول لا يركز على أدوات ومنصات ومواقع شبكية وبرمجيات أو مصادر محددة خاضعة للتغيير، بل على المبادئ والإجراءات الأساسية التي ينبغي أن توجه دفة التحقيقات المفتوحة المصدر.

10- وأُعدَّ هذا البروتوكول لتوحيد الإجراءات وتقديم ارشادات منهجية عبر التحقيقات والمؤسسات والسلطات القضائية المتباينة لمساعدة المحققين المتخصصين في المصادر المفتوحة على فهم أهمية العناصر التالية:

(أ) تتبّع مصدر المحتوى المنشور على الإنترنت ونسبه إلى مصدره الأصلي، حيثما أمكن ذلك؛

(ب) تقييم مصداقية المصادر عبر الإنترنت وموثوقيتها؛

(ج) التحقق من المحتوى المنشور على الإنترنت وتقييم صحته وموثوقيته؛

(د) الامتثال للمتطلبات القانونية وللمعايير الأخلاقية؛

(هـ) تقليل أي احتمال بإلحاق الضرر بالمحققين وبمنظماتهم وبالآخرين؛

(و) تعزيز حماية حقوق الإنسان المتعلقة بالمصادر، بما في ذلك الحق في الخصوصية.

باء- الجمهور المستهدف

11- يشمل الجمهور الذي يستهدفه البروتوكول الأفراد والمنظمات الذين يحددون المعلومات المفتوحة المصدر ويجمعونها ويحفظونها و/أو يحللونها بغرض التحقيق في الجرائم الدولية أو انتهاكات حقوق الإنسان لأغراض ضمان العدالة والمساءلة. ويشمل ذلك المحققين والمحامين وأمناء المحفوظات والمحللين العاملين في المحاكم الجنائية الدولية والإقليمية والمختلطة والوحدات الوطنية المعنية بجرائم الحرب ولجان التحقيق وبعثات تقصّي الحقائق وآليات التحقيق المستقلة والمنظمات الدولية وآليات العدالة الانتقالية والمنظمات غير الحكومية. وتتمثَّل الجهات الأخرى التي يمكن أن تستفيد من ذلك في من يعملون في خدمة آليات دولية وإقليمية شتى تجُري تحقيقات قضائية وشبه قضائية مفتوحة المصدر في انتهاكات القانون الدولي[8]. ويؤمل أن يكون البروتوكول مفيداً أيضاً للمستجيبين الأوائل الرقميين، مثل المنظمات المجتمعية والباحثين المستقلين وهم أول من ينشرون في الغالب النتائج المستندة إلى معلومات مفتوحة المصدر ويؤدي عملهم، في أحيان كثيرة، دوراً رئيسياً في إنشاء تحقيقات أخرى مفتوحة المصدر مأذون بها رسمياً. ويشمل الجمهور المستهدف أيضاً الأفراد والمنظمات الذين يدعمون الضحايا في رفع دعاوى مدنية على فرادى الجناة أو الدول. وبوجه عام، قد يكون البروتوكول معيناً لمن يستنتجون استنتاجات وقائعية أو قانونية مستندة إلى التحقيقات المفتوحة المصدر بتمكينهم بشكل أفضل من تقييم محتوى أي تحقيقات مفتوحة المصدر يعتمدون عليها أو يقيِّمونها.

12- ويندرج في عداد أصحاب المصلحة المحتملين الآخرين مقدمو الخدمات على شبكة الإنترنت، مثل منصات التواصل الاجتماعي، التي تُخزِّن كميات كبيرة من البيانات ويمكن أن تقوم بدور رئيسي في الحفاظ على البيانات والمطورون الذين يقدمون برمجيات لتعزيز تقنيات التحقيق المفتوحة المصدر وعملياته.

جيم- التعاريف

13- لإتاحة معايير وإرشادات عملية للتحقيقات المفتوحة المصدر، يجب أن يكون لدى المحققين فهم مشترك لمصطلحات بعينها. وفي هذا الفرع، نُوضِّح المصطلحات الرئيسية المستخدمة في هذا البروتوكول برمته ويشمل ذلك التمييز بين المصطلحات التي يُخلط بينها بشكل شائع[9].

1- المعلومات المفتوحة المصدر مقابل المعلومات المغلقة المصدر

14- تشمل المعلومات المفتوحة المصدر المعلومات المتاحة للجمهور التي يمكن لأي فرد من أفراده ملاحظتها أو ابتياعها أو طلبها دون حاجة إلى وضع قانوني خاص أو اللجوء إلى النفاذ إليها بشكل غير مأذون به. أما المعلومات المغلقة المصدر، فهي المعلومات التي يخضع الاطلاع عليها لقيود أو لحماية القانون[10]، ولكن يمكن الحصول عليها بشكل

(8) انظر، على سبيل المثال، البلاغات وتقارير الزيارات الصادرة عن الإجراءات الخاصة لمجلس حقوق الإنسان. يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/ar/hrbodies/sp/pages/welcomepage.aspx. انظر أيضاً أعمال لجان الجزاءات التي أنشأها مجلس الأمن. يمكن الاطلاع عليه في الرابط التالي: www.un.org/securitycouncil/ar/content/repertoire/sanctions-and-other-committees.

(9) للاطلاع على تجميع أكثر شمولا لِلمصطلحات والتعاريف ذات الصلة، انظر الفصل الثامن.

(10) على سبيل المثال، المعلومات المميزة والمعلومات السرية.

قانوني من خلال قنوات خاصة، مثل الإجراءات القضائية، أو تقديمها طواعية. وعلى الرغم من بساطة تعريف المعلومات المفتوحة المصدر، فإنَّ تحديد العناصر التي تشكِّل هذه المعلومات أكثر تعقيداً مما يبدو لأول وهلة في سياق المحتوى المنشور على الإنترنت. ويوجد على الإنترنت كم ما برح يزداد من البيانات المنشورة دون موافقة مالكيها، مثل المعلومات المخترقة أو المسربة أو المكشوفة بسبب ثغرات أمنية أو لقيام طرف ثالث بنشرها دون الحصول على الأذونات الملائمة. وعلى الرغم من أنَّ هذه المعلومات متاحة للجمهور، وبالتالي فهي تُعد مفتوحة المصدر من الناحية التقنية، فقد تكون هناك قيود قانونية وأخلاقية مفروضة على أنواع بعينها من الاستخدام النهائي. وعلاوة على ذلك، قد تكون المعلومات الرقمية في متناول ذوي المهارات والتدريب التقنيين المتخصصين الذين يستطيعون النفاذ إلى الشبكات والاطلاع على بيانات يتعذر على الشخص العادي النفاذ إليها، أو لا يرجح نفاذه إليها[11]. ومن الأمثلة على ذلك، المعلومات التي يمكن الحصول عليها من الشبكة الخفية – أي ذلك الجزء من الإنترنت الذي لا يُنفذ إليه إلا ببرمجيات معينة، مثل متصفح Tor[12]. ولئن كانت الشبكة الخفية تتيح إخفاء الهوية، وهي ميزة جعلت منها مكاناً جذاباً للنشاط غير القانوني، فإنَّ استخدام متصفح Tor والبحث في الشبكة الخفية يعتبران أمراً قانونياً في معظم البلدان. ويدرج البروتوكول هذه المعلومات في نطاق "المصدر المفتوح" في الحالات التي لا يوجد نفاذ غير مصرح به إلى المعلومات. وأوضح تمييز هو أنَّ المعلومات المفتوحة المصدر لا تنطوي على التفاعل مع فرادى مستخدمي الإنترنت أو التماس معلومات منهم[13]. ويُعدُّ الحصول على المعلومات من مستخدمي الإنترنت الآخرين من خلال الاتصال بهم مصدراً مغلقاً.

15- والمعلومات الرقمية مفتوحة المصدر[14] هي معلومات مفتوحة المصدر منشورة على الإنترنت ويمكن النفاذ إليها، على سبيل المثال، على مواقع الشبكة العامة، أو قواعد بيانات الإنترنت، أو منصات التواصل الاجتماعي. وترد في ما يلي سبل مختلفة للحصول على معلومات مفتوحة المصدر.

2- الحصول على معلومات رقمية مفتوحة المصدر

(أ) ملاحظة

16- يمكن الحصول على المحتوى المنشور على العديد من المنصات ببساطة بالانتقال إلى موقع ذي صلة باستخدام أي عدد من متصفحات الشبكة المجانية. وتتطلب المنصات الأخرى عبر الإنترنت من المستخدمين تسجيل الدخول أو التسجيل من أجل النفاذ إلى المحتوى وعرضه. ويُعد هذا المحتوى مفتوح المصدر طالما ظلَّت هذه العمليات مفتوحة لجميع المستخدمين في الولايات القضائية التي يكون فيها النفاذ قانونياً، ولم تُنتهك أي ضوابط تتعلق بالخصوصية، أو بالأمن عند النفاذ إلي المحتوى، أو عرضه. ومع ذلك، قد لا يكون بعضٌ من المحتوى المستوفي لهذا التعريف مصدراً مفتوحاً. وتشمل الأمثلة على ذلك المعلومات المميزة، أو السرية، أو المحمية قانوناً بطريقة أخرى. وفي هذه الحالات، ومع أنَّ بإمكان أي فرد من أفراد الجمهور ملاحظة المعلومات، فإن استخدامها كدليل في الإجراءات القضائية قد يخضع لقيود. وقد يثير الاعتماد على هذه المواد أيضاً مخاوف أخلاقية أو منهجية، مثل العجز عن إسناد المحتوى إلى مصدره، أو التحقق منه.

(ب) الشراء

17- توجد مصادر بيانات عديدة تتعلق بتحقيقات مفتوحة المصدر على منصات تقتضي دفع مقابل، أو تتكون من نموذج مختلط يجمع بين المجانية ودفع مبلغ من المال لقاء وظائف إضافية ومقابل الحصول على البيانات. ويوجد عدد متزايد من الشركات التي تجمع البيانات العامة وتقدم خدمات مجانية ومدفوعة الأجر للحصول على تلك البيانات. وسيجد المحققون المتخصصون في المصادر المفتوحة بيانات كثيرة مفيدة في قواعد بيانات وعلى منصات لا يمكن النفاذ إليها إلا بعد تخطي حواجز الدفع. ولأغراض هذا البروتوكول، تشمل المعلومات المفتوحة المصدر الخدمات المدفوعة الأجر المتاحة لجميع أفراد الجمهور، ولكنها لا تتضمن الخدمات التي تقتصر إمكانية النفاذ إليها على مجموعات

(11) قد تنتهك بعض الإجراءات شروط خدمة موقع على شبكة الإنترنت، ولكنها لا تكون غير قانونية في حد ذاتها. فعلى سبيل المثال، يُعد انتهاك شروط خدمة موقع شبكي لاستخراج البيانات سلوكاً غير مأذون به قد يؤدي إلى الحرمان من استخدام الموقع الشبكي.

(12) تشير الشبكة الخفية إلى ذلك الجزء من الإنترنت الذي لا يمكن النفاذ إليه إلا باستخدام برمجيات متخصصة. ومتصفح Tor هو أحد الأمثلة على هذه البرمجيات.

(13) لئن كان شراء معلومات من قاعدة بيانات خاصة أو تقديم طلب للحصول على معلومات من وكالة حكومية عامة يتطلب درجة معينة من التبادل عبر الإنترنت، فإنه غالباً ما يكون عملية آلية ويختلف عن نوع التفاعل مع فرادى مستخدمي الإنترنت الآخرين المذكورين هنا.

(14) يمكن أيضاً أن يُشار إلى المعلومات المفتوحة المصدر بأنها تمثل محتوى منشوراً على الإنترنت، أو مواد منشورة على الإنترنت، أو بيانات معروضة على الإنترنت في البروتوكول.

بعينها، مثل الموظفين المكلفين بإنفاذ القوانين، أو المحققين الخاصين المأذون لهم بذلك.

(ج) الطلب

18- في هذا السياق، يشير مصطلح "الطلب" إلى الطلبات التي يقدمها أي فرد للحصول على معلومات عامة من وكالات الدولة بموجب قوانين حرية المعلومات أو إتاحة النفاذ إليها. ولا يشير هذا المصطلح إلى الطلبات المقدمة إلى الأفراد، أو الشركات، أو المنظمات لتسليم ما لديهم من معلومات طوعاً، بل يقتصر على الطلبات المقدمة إلى كيانات الدولة التي تقع عليها التزامات قانونية بالرد بالطريقة نفسها على جميع الأشخاص. ويمكن أن تؤدي التحقيقات المفتوحة المصدر إلى أنشطة تحقيق أخرى عبر الإنترنت، مثل التواصل مع مصادر خارجية باستخدام خدمات المراسلة، أو غرف التحادث، أو المنتديات، أو البريد الإلكتروني. ويتجاوز هذا التواصل نطاق التحقيق المفتوح المصدر الذي يتناوله هذا البروتوكول.

3- الاستخبارات المفتوحة المصدر

19- تشير الاستخبارات المفتوحة المصدر إلى فئة فرعية من المعلومات المفتوحة المصدر تُجمع وتستخدم لغرض محدد هو الاستعانة بها في وضع السياسات واتخاذ القرارات، وغالباً ما يكون ذلك في سياق عسكري أو سياسي. وبينما تشمل المعلومات المفتوحة المصدر جميع المعلومات المتاحة للجمهور التي يمكن لأي شخص الحصول عليها بشكل قانوني، تمثل الاستخبارات المفتوحة المصدر مجموعة فرعية من تلك المعلومات "التي يتم جمعها واستغلالها ونشرها في الوقت المناسب على جمهور ملائم لغرض الإيفاء بشرط استخباراتي محدد"[15]. وتستخدم الاستخبارات المفتوحة المصدر بحسبانها معلومات أساسية لأغراض اتخاذ القرارات ضمن سياق القضايا الجنائية الدولية وقضايا حقوق الإنسان – على سبيل المثال للاستعانة بها في أنشطة متعلقة بالأمن، مثل حماية الشهود وأعضاء الفريق الذين يذهبون إلى الميدان، أو تعقب أشخاص مثيرين للاهتمام – بدلاً من وظائف جمع المعلومات المتعلقة بعمليات التحقيق، مثل تحديد عناصر الجرائم المختلفة.

4- التحقيق المفتوح المصدر

20- يشير التحقيق المفتوح المصدر إلى استخدام معلومات مفتوحة المصدر في وظائف جمع المعلومات والأدلة.

5- الأدلة المفتوحة المصدر

21- ينبغي التمييز بين مصطلح "الأدلة" ومصطلح "المعلومات"[16]. وفي جميع الولايات القضائية، تُعرَّف الأدلة بأنها عملية إثبات للواقعة (الوقائع) تُستخدم في تحقيق، أو في جلسة استماع لدعوى، مثل المحاكمة. وتعني الأدلة المفتوحة المصدر معلومات مفتوحة المصدر ذات قيمة إثباتية يمكن قبولها لإثبات الوقائع في الإجراءات القانونية. ومن المهم تفادي سوء استخدام مصطلح "الأدلة" أو الإفراط في استخدامه عند الإشارة إلى "المعلومات" بشكل عام.

6- المعلومات المفتوحة المصدر مقابل البرمجيات المفتوحة المصدر

22- غالباً ما يُستخدم مصطلح "المصدر المفتوح" لوصف البرمجيات أو الشفرات المتاحة مجاناً للاستخدام وإعادة النشر، دون قيود بشأن حقوق الطبع والنشر، أو براءات الاختراع، أو غيرها من الضوابط القانونية. وتبنى البرمجيات المفتوحة المصدر من شفرة مصدرية بوسع أي شخص لديه حق النفاذ فحصها وتعديلها وتحسينها[17]. وهي عادة ما تكون غير مرئية للمستخدمين ولكن يمكن تعديلها وتكييفها بواسطة مبرمج حواسيب. ويمكن تمييز البرمجيات المفتوحة المصدر عن المعلومات المفتوحة المصدر – وإن كانت البرمجيات والأدوات المفتوحة المصدر تُستخدم بشكل متكرر من قبل المحققين المتخصصين في المصادر المفتوحة للعثور على معلومات مفتوحة المصدر وجمعها وحفظها وتحليلها.

7- المصداقية مقابل الموثوقية

23- عندما يتعلق الأمر بأدلة الشهادات في المحاكمات الجنائية الدولية، يُقيِّم القضاة "مصداقية الشاهد" و"موثوقية شهادته"[18]. وفي التحقيقات التي تجريها لجان التحقيق ولجان تقصي الحقائق التابعة للأمم المتحدة والتحقيقات

(15) National Open Source Enterprise, Intelligence Community Directive No. 301, 11 July 2006, p. 8 (حذفت الحاشية).

(16) Federica D'Alessandra and others, eds., Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices (The Hague, Public International Law and Policy Group, 2016), p. 17.

(17) انظر Opensource.com، "What is open source?".

(18) انظر المحكمة الجنائية الدولية، *المدعي العام ضد بوسكو نتاغاندا*، القضية رقم ICC-01/04-02/06، الحكم المؤرخ 8 تموز/يوليه 2019، الفقرة 53.

المماثلة لذلك، تنص الارشادات على أنَّ "مجري المقابلة ينبغي أن يُقيِّم مصداقية من تُجرى معه المقابلة وموثوقيته"[19]. وتضيف الإرشادات أنَّ "التقييم سينظر في مدى وجاهة المعلومات في سياق موضوع التحقيق. وسينظر أيضاً في موثوقية المصدر وصحة المعلومات أو صدقها"[20]. ويستخدم البروتوكول هذه المصطلحات على النحو التالي:

(أ) تشير "المصداقية" إلى الصدقية أو الجدارة بالثقة؛

(ب) تشير "الموثوقية" إلى القدرة على الأداء بشكل متسق أو موثوق به أو على النحو المتوقع؛

(ج) تشير "الصدقية" أو "الصلاحية" إلى الدقة أو الصدق أو التوافق مع الحقائق.

(19) مفوضية الأمم المتحدة السامية لحقوق الإنسان، لجان التحقيق وبعثات تقصي الحقائق بشأن القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني: التوجيه والممارسة (نيويورك وجنيف، 2015)، الصفحة 52. يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/sites/default/files/Documents/Publications/CoI_Guidance_and_Practice_AR.pdf.

(20) المرجع نفسه، الصفحة 59.

ثانياً

المبادئ

ملخص الفصل

- للامتثال للمبادئ المهنية المتعلقة بالتحقيقات الرقمية المفتوحة المصدر، ينبغي على المحققين الحرص على أن يكونوا مسؤولين وأكفاء وموضوعيين وعلى أن يتم عملهم وفقاً للقانون ومع إيلاء الاعتبار الواجب للشواغل الأمنية.
- يجب على المحققين أيضاً النظر في الأساليب التي يستخدمونها في جميع مراحل تحقيقاتهم. وتشمل المبادئ المنهجية، كحد أدنى، الدقة وتقليل البيانات إلى أدنى حد وعرض البيانات ومراعاة أمنها في التصميم.
- ختاماً، ينبغي أن يسترشد جميع المحققين بالاعتبارات الأخلاقية. وتشمل هذه الاعتبارات، كحد أدنى، حماية كرامة جميع الأفراد الذين يشاركون في التحقيق أو تكون لهم صلة به، فضلاً عن توخي التواضع والشمول والاستقلالية والشفافية.

24- لئن كانت التكنولوجيات والأدوات والتقنيات المستخدمة في التحقيقات المفتوحة المصدر تتغير، فإنَّ بعض المبادئ المنهجية والأخلاقية الشاملة ينبغي أن تُكرّس. ويُعد تحديد هذه المبادئ خطوة هامة نحو إضفاء الطابع المهني على مجال التحقيقات المفتوحة المصدر. وتُعد المبادئ التالية أساسية لضمان جودة التحقيقات المفتوحة المصدر التي ستعزز من جانبها مصداقية هذه التحقيقات وموثوقيتها وفائدتها المحتملة لضمان المساءلة وتقليل الضرر الذي يحتمل أن يصيب مختلف أصحاب المصلحة.

ألف- المبادئ المهنية

1- المساءلة

25- يجب أن يكون المحققون المتخصصون في المصادر المفتوحة مسؤولين عن أفعالهم، وهو أمر يمكن تحقيقه، في كثير من الأحيان، بالتوثيق وحفظ السجلات والرقابة بشكل واضح. وتمثّل الشفافية في أساليب التحقيق وإجراءاته عنصراً أساسياً لتحقيق المساءلة. ومن ثم، ينبغي للمحققين المتخصصين في المصادر المفتوحة أن يحتفظوا بسجلات عن أنشطتهم، كلما كان ذلك مستطاعاً ومعقولاً. وينبغي توثيق خطوات التحقيق المفتوح المصدر توثيقاً واضحاً ومتسقاً خلال مراحل تحديد المواد ذات الصلة وجمعها وتحليلها والإبلاغ عنها. وينبغي لأي أفراد يشاركون في جمع المعلومات، أو التعامل معها على الإنترنت، أن يكونوا على علم بأنَّ المنهجية التي يتبعونها قد تكون موضع مساءلة قد تشمل استدعاءهم للإدلاء بشهاداتهم في المحاكمة. ويمكن توثيق التحقيقات المفتوحة المصدر يدوياً أو باستخدام عمليات آلية تتيحها برمجيات مختلفة. ويمكن استخدام الطرق اليدوية أو الآلية طالما كانت الوثائق متسقة وشاملة بالقدر الكافي. وينبغي للمستخدمين أن يفهموا العمليات والبرمجيات الآلية التي يتوخى فيها أن تكون قابلة للتوضيح في المحكمة، إما من قبل مستخدميها أو من وضعوها. وفضلاً عن ذلك، حري بالمحققين المتخصصين في المصادر المفتوحة تسجيل أي أدوات أو برمجيات تُستخدم في إطار عملهم.

2- الكفاءة

26- يجب أن يكون المحققون المتخصصون في المصادر المفتوحة قد تلقوا تدريباً مناسباً وأن يتمتعوا بمهارات تقنية ملائمة لتنفيذ الأنشطة التي يضطلعون بها. ويجب عليهم الاضطلاع بالأنشطة عبر الإنترنت بشكل مهني وأخلاقي وتجنب الاستيلاء على عمل الآخرين والاعتراف بدور جميع من يشاركون في التحقيق (عندما يكون ذلك آمناً وحين يرغب المشاركون في ذلك) والإبلاغ الدقيق عن البيانات، بما في ذلك الاعتراف بأي ثغرات قد تشوب المحتوى المنشور على الإنترنت. ويجب أن يتحلى المحققون وعمليات التحقيق المفتوحة المصدر بالمرونة وأن يظلوا مطلعين على الدوام على التطورات الجديدة وأن يعتمدوا تكنولوجيات وتقنيات جديدة حسب الاقتضاء. وبالإضافة إلى ذلك، ينبغي أن يكون لدى منظمات وأفرقة التحقيق آليات للتحقق من تنفيذ الإجراءات والتقيد بها بانتظام.

3- الموضوعية

27- الموضوعية مبدأ أساسي ينطبق على جميع التحقيقات، سواء استُخدمت فيها الإنترنت أو لم تُستخدم. ويجدر بالمحققين المتخصصين في المصادر المفتوحة أن يدركوا أنَّ التحيز الشخصي والثقافي والهيكلي قد يؤثر سلباً في عملهم وأن ثمة حاجة إلى اتخاذ تدابير مضادة حرصاً على الموضوعية. ويجب على المحققين المتخصصين في المصادر المفتوحة الحرص على الموضوعية في تحقيقاتهم ووضع فرضيات عمل متعددة واستخدامها وعدم تفضيل أي نظرية معينة لشرح قضاياهم. وتكتسي الموضوعية أهمية خاصة في التحقيقات المفتوحة المصدر التي تُجرى عبر الإنترنت بسبب طريقة تنظيم المعلومات على الإنترنت وتقديمها للمستخدمين. فقد يؤدي استخدام متصفح أو محرك بحث أو مصطلحات بحث أو تركيب الى نتائج مختلفة تمام الاختلاف حتى وإن لم يتغير الاستقصاء الأساسي. وقد تنال أشكال التحيز المتأصلة في بنية الإنترنت وفي الخوارزميات التي تستخدمها محركات البحث والمواقع الشبكية من موضوعية نتائج البحث[21]. وقد تتأثر نتائج البحث أيضاً بعوامل تقنية عديدة، من بينها الجهاز المستخدم وموقعه وسجل البحث السابق للمستخدم ونشاطه على الإنترنت. وينبغي للمحققين المتخصصين في المصادر المفتوحة موازنة هذه التحيزات بتطبيق منهجيات تكفل أن تكون نتائج البحث متنوعة قدر الإمكان، على سبيل المثال، بإجراء استقصاءات بحث متعددة واستخدام مجموعة متنوعة من محركات البحث والمتصفحات[22]. وينبغي أن يدرك المحققون أنَّ نتائج البحث قد تتأثر أيضاً بعوامل أخرى لأسباب من بينها التباين في البيئة الرقمية، فقد تكون المعلومات المنشورة على الإنترنت متاحة

(21) انظر Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, New York University Press, 2018); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York, Picador, 2019).

(22) انظر على سبيل المثال Paul Myers, "How to conduct discovery using open source methods", in *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020) (يناقش الطرق التي يؤثر بها اختيار محركات البحث ومصطلحات البحث في انحياز نتائج التحقيق المفتوح المصدر).

بشكل متفاوت من مجموعات أو شرائح معينة من المجتمع[23]. وفي نهاية المطاف، ينبغي للمحققين السعي دائماً إلى أن يكونوا على دراية بما لديهم، عن وعي أو غير وعي، من ضروب التحيز وأن يعملوا على تداركها[24].

4- الصبغة القانونية

28- ينبغي أن تمتثل التحقيقات المفتوحة المصدر للقوانين المعمول بها. ويعني ذلك أنَّ المحققين ينبغي أن يكون لديهم فهم أساسي للقوانين التي تنطبق على عملهم. وعلى وجه الخصوص، ينبغي أن يكون المحققون على دراية بقوانين حماية البيانات والحق في الخصوصية الذي يحميه القانون الدولي لحقوق الإنسان[25]. وعلى الرغم من أنَّ المعلومات قد تكون متاحة للجمهور، فإنَّ هذا لا يعني أنَّ جمعها واستخدامها لن يكون لهما تأثير في الخصوصية. ويجب على المحققين المتخصصين في المصادر المفتوحة مراعاة تبعات أفعالهم على الخصوصية، بما في ذلك الخصوصية التي يتوقعها الشخص بشكل معقول في الفضاءات الرقمية المختلفة. وحري بالمحققين أن يكونوا أيضاً على دراية بتأثير الفسيفساء، فالبيانات العامة، وإن كانت مجهولة المصدر، قد تكون عرضة لإعادة تحديد الهوية إن نُشرت مجموعات كافية من البيانات تتضمن معلومات مماثلة أو مكملة، أو لو جُمعت هذه المعلومات مع بعضها[26]. وبالإضافة إلى ذلك، ينبغي أن يدرك المحققون أنَّ الرصد المستمر والمتواصل للأفراد على الإنترنت، أو جمع البيانات الشخصية بانتظام والاحتفاظ بها في الأجل الطويل، قد يتطلب، في بعض الولايات القضائية، الحصول على أذونات وضمانات

(23) انظر على سبيل المثال Alexa Koenig and Ulic Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes", in *Technologies of Human Rights Representation*, James Dawes and Alexandra S. Moore, eds. (forthcoming). (يناقش كيف يمكن أن يقلل النقص النسبي في استخدام النساء للهواتف الذكية واستخدام لغة مشفرة على الإنترنت من قبل الناجين من العنف الجنسي والعنف الجنساني من كمية المعلومات المفتوحة المصدر المتعلقة بهذه الجرائم وإمكانية الحصول عليها – وكيف أنَّ كثرة الرجال في كل من المناصب التكنولوجية وكمحققين في جرائم الحرب قد تؤثر سلباً في احتمال أن تنتج عمليات الكشف الآلية و/أو اليدوية معلومات مفتوحة المصدر عن الجرائم الجنسانية). ولمزيد من المناقشة بشأن التحيز، انظر الفصل الثاني–جيم أدناه بشأن المبادئ الأخلاقية والفصل الخامس–باء أدناه بشأن تقييم المشهد الرقمي).

(24) انظر على سبيل المثال Forensic Science Regulator, *Cognitive Bias Effects Relevant to Forensic Science Investigations, FSR-G-217* (Birmingham, United Kingdom, 2015) (يناقش فئات مختلفة من التحيز المعرفي الذي يمكن أن يؤثر سلباً في جودة التحقيق، بما في ذلك التحيز في التوقعات والتحيز التأكيدي والترسيخ والتحيز السياقي والتأثيرات الناشئة عن الدور وإعادة التشكيل)؛ Wayne A. Wallace, *The Effect of Confirmation Bias on Criminal Investigative Decision Making* (Minneapolis, Walden University ScholarWorks, 2015) (يشرح التحيز التأكيدي بحسبانه عملية يبحث من خلالها المحققون عن المعلومات التي تدعم نظريتهم المفضلة في القضية أو يصدقون تلك المعلومات "مع تجاهل أو تبرير الأدلة التي تدحض التأكيد")؛ Jon S. Byrd, bias, ethics, and mistakes in forensics", Forensic Pathways, 21 March 2020؛ Michael Pittaro, "Implicit bias within the criminal justice system", Psychology Today, 21 November 201 انظر أيضاً Yvonne McDermott, Daragh Murray and Alexa Koenig, "Digital accountability symposium: whose stories get told, and by whom? Representativeness in open source human rights investigations", Opinio Juris, 19 December 2019 (يناقش كيف يمكن أن تؤثر أساليب التحقيقات المفتوحة المصدر سلباً في "أنواع الانتهاكات المبلغ عنها والضحايا والشهود الذين تتاح لهم الفرصة لإسماع أصواتهم وكيفية بناء روايات الانتهاكات الجماعية لحقوق الإنسان")؛ والمشروع الذي تقوده إيفون ماكديرموت بعنوان "The future of human rights investigations: using open source intelligence to transform the documentation and discovery of human rights violations".

(25) تنص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه لا يجوز تعريضُ أحد لتدخُّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حقٌّ في أن يحميه القانونُ من مثل ذلك التدخُّل أو تلك الحملات وينص العهد الدولي الخاص بالحقوق المدنية والسياسية في المادة 17 منه على أنه لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو أسرته أو بيته أو مراسلاته ولا لأي حملات غير قانونية تمس شرفه أو سمعته. وتنص المادة 17 أيضاً على أن من حق كل شخص أن يحميه القانون من هذا التدخل أو المساس.

(26) "يستمد مفهوم تأثير الفسيفساء من نظرية الفسيفساء لجمع المعلومات التي تشير إلى أنَّ أجزاء متفرقة من المعلومات تصبح، وإن كانت محدودة الفائدة منفردة، مهمة عند جمعها مع أنواع أخرى من المعلومات (Pozen 2005). ويشير مفهوم تأثير الفسيفساء، عند تطبيقه على بيانات الاستخدام العام، إلى أنّ البيانات، حتى وإن كانت مجهولة المصدر وتبدو غير مفيدة بمعزل عن غيرها، قد تصبح عرضة لإعادة تحديد الهوية إن نُشر ما يكفي من مجموعات البيانات التي تتضمن معلومات مماثلة أو تكميلية". انظر John Czajka and others, *Minimizing Disclosure Risk in HHS Open Data Initiatives* (Washington, D.C., Mathematica Policy Research, 2014), appendix E, p. E-7. يمكن الاطلاع عليه في الرابط التالي: https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. انظر أيضاً David E. Pozen, "The mosaic theory, national security, and the Freedom of Information Act", Yale Law Journal, vol. 115, No. 3 (December 2005), pp. 628-679.

إضافية بسبب ازدياد المخاوف التي تثيرها هذه الأنشطة بشأن الخصوصية[27].

5- الوعي الأمني

29- في حين تتناول مراعاة الأمن في التصميم[28] بنية التحقيق وبنيته التحتية وأي أنشطة جانبية، يركز مبدأ الوعي الأمني على الاعتبارات التي يجب على الأفراد مراعاتها أثناء عملهم – ومن أهمها الوعي بسلوكهم على الإنترنت. ويجب أن يتمتع جميع الأفراد الذين يجرون تحقيقات عبر الإنترنت بوعي أمني تشغيلي أساسي لتقليل أثرهم الرقمي إلى الحد الأدنى وأن يكونوا مدركين للأخطار المحتملة. وينبغي للمنظمات التي تجري تحقيقات مفتوحة المصدر أن تزود محققيها بالتدريب على أمن المعلومات حتى يدركوا الأخطار التي قد يواجهونها ويفهمون الركائز الأساسية الثلاث لأمن المعلومات وهي: (أ) السرية (مثل السماح للمستخدمين المأذون لهم فقط بالنفاذ إلى البيانات)؛ (ب) سلامة البيانات (ضمان عدم العبث بالبيانات أو تغييرها بطريقة أخرى من قبل مستخدمين غير مأذون لهم بذلك)؛ و(ج) الإتاحة (التحقق من إتاحة النظم والبيانات للمستخدمين المصرح لهم بذلك عندما يحتاجون إليها). وينبغي أن يركز التدريب أيضاً على هيكل حوكمة الإنترنت. وينبغي إجراء عمليات تقييم للتهديدات والأخطار قبل الشروع في أنشطة التحقيق عبر الإنترنت، واستعراضها وتعديلها دورياً حسب الاقتضاء. وتقع مسؤولية الأمن على عاتق الجميع ولا تقتصر على وحدات تكنولوجيا المعلومات أو مديري الأخطار الأمنية فحسب.

باء- المبادئ المنهجية

1- الدقة

30- ثمة ضرورة منهجية وأخلاقية لضمان دقة التحقيقات – ومن ثم جودتها – بالاعتماد حصراً على مواد موثوق بها. ويجدر بالمحققين المتخصصين في المصادر المفتوحة أن يتحروا، ما استطاعوا إلى ذلك سبيلاً، الصدق والدقة في تحقيقاتهم وفي عرض أي نتائج خاصة فيما يتعلق بالاعتراف بمواطن الضعف في البيانات الأساسية أو في القضية ككل. وغالباً ما يتحقق المزيد من الدقة باستخدام فرضيات عمل متعددة واختبارها و/أو مراجعتها من قبل الأقران، وكلاهما يمكن أن يعين على تقليل فرص اختيار البيانات وتفسيرها وعرضها بشكل متحيز. وينبغي تجنب الغلو في الاستنتاجات التحليلية أو المبالغة فيها. ومن شأن استخدام لغة واضحة وموضوعية وقائمة على الحقائق وتجنب اللغة العاطفية أن يصون موضوعية التحقيق ونتائجه الفعلية والمتصورة.

2- تقليل البيانات إلى الحد الأدنى

31- ينص مبدأ تقليل البيانات إلى أدنى حد على ألا تُجمع المعلومات الرقمية وتُعالج إلا إذا كانت: (أ) مبررة لغرض واضح؛ (ب) ضرورية لتحقيق ذلك الغرض؛ (ج) متناسبة مع القدرة على تحقيق ذلك الغرض[29]. وفي سياق التحقيقات المفتوحة المصدر، ينبغي ألا يُجمع المحتوى المنشور على الإنترنت إلا إن كانت له صلة بتحقيق بعينه. ويرجِّح هذا المبدأ كفة جمع المعلومات يدوياً وبشكل مفصل على جمعها آلياً وبكميات كبيرة، مع الأخذ في الحسبان أنَّ طريقة الجمع الأخيرة هذه قد تكون مناسبة في بعض الحالات. وفي تطبيق هذا المبدأ على جمع المحتوى المنشور على الإنترنت ما يعين على تجنب الإفراط في جمع البيانات، وهو أمر مهم لعدة أسباب. وتشكل المغالاة في جمع البيانات مصدر قلق خاص عند استخدام عمليات الجمع الآلي، فهو يحدث ثغرات أمنية أو يفاقمها[30]، لا سيما إن كان سبباً في ألاَّ يدرك المحققون ما في حوزتهم من أنواع المعلومات. وقد تثير المغالاة في جمع المعلومات أيضاً مخاوف تتعلق بالخصوصية وحماية البيانات إن كانت العملية الآلية لا تميز بين أنواع المحتوى. وختاماً، يحقق تجنب المغالاة في جمع البيانات الأغراض العملية المتمثلة في تقليل تكاليف التخزين إلى أدنى حد ومنع الاختناقات في نهاية كل مرحلة من مختلف مراحل دورة التحقيق، مثل المراجعة والتحليل والإفصاح عن البيانات إن أفضى التحقيق إلى إجراءات قانونية.

(27) على سبيل المثال في المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية، ينص القانون على أنَّ "البيانات الشخصية المستخدمة لاغراض ... إنفاذ القانون يجب ألا يُحتفظ بها لفترة تزيد عن المدة اللازمة للغرض الذي استُخدمت من أجله" (الفصل 12 من قانون حماية البيانات لعام 2018، الجزء 3، الفصل 3، القسم 39(1)). وبموجب اللائحة 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 نيسان/أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، وإلغاء التوجيه 95/46/EC (اللائحة العامة لحماية البيانات)، لا يمكن جمع البيانات الشخصية إلا "لأغراض محددة وصريحة ومشروعة" ويجب أن تقتصر على المعلومات اللازمة للغرض الذي جمعت من أجله وأن تظل قابلة للتحديد فقط ما دامت ضرورية لأغراض الجمع (المادتان 5 و6).

(28) انظر الفقرة 33 أدناه.

(29) استمد البروتوكول مبدأ تقليل البيانات إلى أدنى حد من لائحة الاتحاد الأوروبي العامة لحماية البيانات، ولكنه كيَّفها لتناسب سياق التحقيق المفتوح المصدر (انظر المادة 5 من اللائحة).

(30) انظر الفصل الرابع أدناه بشأن الأمن للاطلاع على أمثلة على مواطن الضعف الأمنية.

3- الحفظ

32- من المهم تفادي قصور جمع المعلومات شأنه في ذلك شأن تجنب المغالاة في جمع المعلومات المفيدة. وقد يثير ذلك قلقاً خاصاً في سياق المعلومات المنشورة على الإنترنت التي تتسم في كثير من الأحيان بعدم الاستقرار من حيث دوامها وتوافرها. وصُمم مبدأ الحفظ لتجنب القصور في جمع البيانات حتى لا تضيع أدلة مفيدة قد تكون ذات قيمة إثباتية. فعلى سبيل المثال، قد تزيل منصات التواصل الاجتماعي محتوى ينتهك شروط الخدمة الخاصة بها حتى وإن كان لهذا المحتوى قيمة محتملة لدى المحققين. وما لم يُقدم طلب حفظ في الوقت المناسب إلى المنصة المعنية أو يُحافظ المحققون على المحتوى بطريقة أخرى، فقد تضيع هذه المعلومات إلى الأبـد. وبالإضافة إلى ذلك، قد يختار المستخدمون حذف المحتوى الخاص بهم أو تعديله، فتصبح معلومات كانت عامة غير متاحة. وعلاوة على ذلك، يمكن بسهولة إخراج المعلومات الموجودة على شبكة الإنترنت من سياقها، أو فقدانها، أو محوها، أو إتلافها. وإن أريد للمواد الرقمية أن تظل متاحة وقابلة للاستخدام في آليات المساءلة في المستقبل، فلا بد من الحفاظ عليها بهمة وعناية في الأجلين القصير والطويل[31].

4- مراعاة الأمن في التصميم

33- يقتضي مبدأ مراعاة الأمن في التصميم أن تكون المعلومات الرقمية والعمليات المجراة عبر الإنترنت آمنة بالضرورة، قدر الإمكان. ويجدر بالهيئات التي تجري تحقيقات مفتوحة المصدر عبر الإنترنت أن تستثمر في التدابير التقنية والهيكلية المناسبة لتكون البنية التحتية بالضرورة – بما في ذلك الأجهزة والبرمجيات – محجوبة الهوية بشكل سليم وغير قابلة لنسبها إلى جهة عندما يستخدم المحققون الإنترنت، وأن تنفذ تلك التدابير. وينبغي أن تحتوي جميع المعدات على برمجيات محدثة للحماية من البرامج الضارة وعلى ترتيبات الخصوصية والأمان المناسبة. وينبغي اتخاذ تدابير أمنية قبل بدء أنشطة التحقيق عبر الإنترنت ورصد هذه التدابير وتحديثها باستمرار وتعديلها حسب الحاجة. وحري بالمحققين، أو فرق التحقيق، أو المنظمات الترتيب لإجراء اختبارات مستمرة تشمل اختبار الاختراق[32]، للتحقق من أنَّ أنظمتهم الامنية تؤدي عملها على النحو المصمم لها.

جيم- المبادئ الأخلاقية

1- الكرامة

34- ينبغي إجراء التحقيقات بوعي وحساسية حيال أي مسائل أساسية تتعلق بالكرامة، ولا سيما المصالح التي يحميها القانون الدولي لحقوق الإنسان. فعلى سبيل المثال، ينبغي للمحققين الالتزام بمبادئ عدم التمييز التي قد تؤثر في من يُحقق معه ومن يُجري التحقيق أو يُعهد إليه بالتحقيق وإدراج ضمانات الأمن الرقمي والبدني والنفسي للشهود والناجين والمحققين الآخرين والمتهمين وغيرهم ممن قد يتأثرون سلباً بذلك. وقد يؤثر الالتزام بمبدأ الكرامة أيضاً في ما يتم مشاركته علناً عن التحقيق، بما في ذلك كتابة وفي شكل أي مواد مرئية – على سبيل المثال، تجنب إظهار مدى المعاناة أو العنف الكامل، إن لم يكن ذلك ضرورياً. ويضمن هذا المبدأ أن تمثل معايير حقوق الإنسان مجموعة توجيهية من المعايير يستعان بها لإجراء تحقيقات أخلاقية مفتوحة المصدر.

2- التواضع

35- يجب أن يتحلى المحققون المتخصصون في المصادر المفتوحة بالتواضع وأن يدركوا أوجه القصور فيهم ويكونوا على وعي بما يجهلون. وقد يتطلب فهم المعلومات المفتوحة المصدر وتفسيرها على نحو سليم تلقي تدريب متخصص أو استشارة الخبراء. ويعني التواضع أيضاً تحمل المسؤولية عن الأخطاء؛ فإن تبيَّن للمحققين أنهم ارتكبوا خطأ، وجب تصحيحه أو الإبلاغ عنه لمن بوسعهم تقليل الضرر الناتج عنه. ومن الناحية المثالية، ينبغي أن توجد آلية للإبلاغ عن الأخطاء وإصدار التصويبات، ولا سيما في حالة التحقيقات العلنية والموزعة على نطاق واسع.

3- الشمول

36- يجب على المحققين المتخصصين في المصادر المفتوحة الحرص على تضمين طائفة من وجهات النظر والخبرات في التحقيقات. وتشمل العوامل التي ينبغي مراعاتها ويحتمل أن تؤثر في الشمول العام لتحقيق عبر الإنترنت نطاق هذا التحقيق الجغرافي والانتهاكات و/أو الجرائم الدولية التي يجري التحقيق فيها والوعي بالطبيعة غير المتكافئة للمعلومات المنشورة على الإنترنت فيما يتعلق بشرائح المجتمع المختلفة[33].

(31) انظر الفصل السادس–دال أدناه بشأن الحفظ للاطلاع على مزيد من التفاصيل.

(32) اختبار الاختراق هو هجوم إلكتروني محاكي تم التصريح به لاختبار أمان النظام.

(33) انظر الفصل الخامس–باء أدناه بشأن تقييم المشهد الرقمي.

وينبغي أيضاً أن تكون أفرقة التحقيق متنوعة تنوعاً يشمل تحقيق توازن جنساني. وبالإضافة إلى ذلك، قد يؤثر مبدأ الشمول، إلى جانب مبدأ الكرامة، في المواد التي يختار المحقق جمعها واستخدامها في التحقيق وأساليب تقديمها إلى فئات مستهدفة مختلفة.

4- الاستقلال

37- ينبغي على المحققين المتخصصين في المصادر المفتوحة حماية أنفسهم وتحقيقاتهم من التأثير غير المناسب. وحري بهم أن يحددوا أي تضارب حقيقي أو متصور في المصالح ويتجنبوه وأن يضعوا ضمانات تخفف من حدة أوجه التضارب التي يتعذر تجنبها. ومن شأن التزام جانب الشفافية في هذه العملية وفي الأساليب والتمويل أن يُيسِّر تقييم الاستقلال وأن يحمي استقلال التحقيق الفعلي والمتصور.

5- الشفافية

38- يتطلب مبدأ المساءلة توخي الشفافية في الأساليب التي يتبعها المحقق وفي النتائج التي يتوصل إليها. أما المبدأ الأخلاقي للشفافية، فيشير إلى كيفية سلوك المحققين المتخصصين في المصادر المفتوحة في الإنترنت وحيال العالم الخارجي. ويعني ذلك تجنب تزييف البيانات[34]. ولئن كان لإخفاء الهوية وعدم الإسناد – بما في ذلك استخدام هويات افتراضية[35] – أهمية لأسباب أمنية، فخليق بالمحققين أن يكونوا على دراية بالتداعيات السلبية المحتملة لتزييف البيانات، مثل الإضرار بسمعة ومصداقية التحقيق أو الفريق أو المنظمة، أو تشويش المعلومات التي جُمعت. وينتهك الحصول على المعلومات من خلال التزييف حق الفرد المستهدف في الخصوصية و/أو يشوه التحقيق، خاصة إن كان التزييف غير قانوني في الولاية القضائية (الولايات) القضائية المعنية.

(34) على سبيل المثال، بمحاولة الانضمام إلى مجموعات مغلقة أو إجراء اتصالات على وسائل التواصل الاجتماعي تحت ذرائع كاذبة.

(35) للاطلاع على مناقشة للهويات الافتراضية، انظر الفصل الرابع–جيم أدناه بشأن الاعتبارات المتصلة بالهياكل الأساسية.

ثالثاً

الإطار القانوني

موجز الفصل

- لتحديد القوانين المنطبقة أهمية بالغة في تقرير ما يجب جمعه وأفضل السبل لذلك. ويختلف ذلك تبعاً لهويات المحققين وهويات أهدافهم والغرض من تحقيقاتهم والولايات القضائية التي يوجدون فيها وتقع فيها الأهداف والبيانات والإجراءات القانونية.
- سيزيد الحفاظ على المواد الرقمية بشكل يصون صحتها ويوثِّق سلسلة الاسناد من احتمال قبولها دليلاً في المحاكم.
- سيحدد نوع التحقيق والهدف النهائي المنشود منه (مثل الإجراءات الجنائية والتقاضي المدني وإجراءات العدالة الانتقالية وما إلى ذلك) عتبة الأدلة التي يتعين تطبيقها.
- قد يؤدي انتهاك حق الفرد في الخصوصية إلى استبعاد الأدلة.

39- يجب على المحققين المتخصصين في المصادر المفتوحة فهم الأطر القانونية التي يعملون فيها. ويشمل ذلك معرفة الهيئات القانونية المنطبقة ذات الصلة بما يجرونه من تحقيقات والأطر القانونية للولايات القضائية التي تُجرى فيها أنشطة التحقيق. ويمكن أن تؤدي المعرفة بالقوانين الموضوعية المنطبقة على التحقيقات، بما في ذلك عناصر الانتهاكات أو الجرائم المحتملة[36]، فضلاً عن أنماط المسؤولية[37]، إلى إجراء تحقيقات أكثر تركيزاً وتعزز احتمال أن تكون المعلومات المجمعة وأي استنتاجات تحليلية مستخلصة منها مفيدة في الجهود الرامية إلى تحقيق العدالة والمساءلة. وبالمثل، ستمكن معرفة القوانين الإجرائية وقواعد الإثبات المعمول بها في الولايات القضائية المعنية المحققين من أداء عملهم بأسلوب يتسق مع متطلبات استخدام المعلومات المفتوحة المصدر في الإجراءات القانونية.

40- وتحدد الصكوك القانونية للمحكمة المختصة أو نظام المحاكم المختص[38] الإطار القانوني بشأن التحقيقات الجنائية الدولية. أما في حالة التحقيقات المأذون بها دولياً، مثل لجان التحقيق، فتحدد الآلية المنشأة لغرض التحقيق، من بين عوامل أخرى، مجموعات القوانين الواجبة التطبيق ونطاق التحقيق جغرافياً وزمنياً[39]. وأما التحقيقات الأخرى، ومن بينها التحقيقات التي تجريها منظمات غير حكومية، فيجوز للكيان الذي يتولى التحقيق أن يحدد بنفسه إطاره القانوني[40].

41- وأُعد هذا الفصل ليستعين به المحققون المتخصصون في المصادر المفتوحة في تقدير الاستخدامات النهائية المحتملة لعملهم وفهمها بشكل أفضل وتكييف أساليب التحقيق التي يتبعونها وفقاً لذلك. وبما أنَّ القوانين المنطبقة تختلف باختلاف الولاية القضائية ونوع التحقيق والسلطة القانونية لكيان التحقيق، تقدم الأفرع التالية لمحة عامة عن الاعتبارات الرئيسية بشأن التحقيق في انتهاكات القانون الدولي المحتملة. ويوصى بأن يحصل المحققون، حيثما أمكن ذلك، على مشورة قانونية متخصصة من محامين مطلعين على الولايات القضائية وعلى الموضوع المعني.

ألف- القانون الدولي العام

42- يركز البروتوكول على ثلاث فئات من القانون الدولي العام تتسم بقدر كبير من التداخل هي: القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان والقانون الجنائي الدولي.

(36) كمثال على ذلك، ينبغي للمحققين، في حالة التحقيق في خطاب الكراهية والتحريض على العنف، أن يفهموا نوع السلوك الذي يصل إلى العتبة العالية للمادة 20(2) من العهد الدولي الخاص بالحقوق المدنية والسياسية. انظر: خطة عمل الرباط بشأن حظر الدعوة إلى الكراهية القومية أو العرقية أو الدينية التي تشكل تحريضاً على التمييز أو العداوة أو العنف (A/HRC/22/17/Add.4، التذييل)، الفقرتان 11 و29، واختبار العتبة القائم على حقوق الإنسان الخاص بها، الذي يمكن الاطلاع عليه بـ 32 لغة. على الموقع التالي: www.ohchr.org/Ar/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx. وفيما يتعلق بخطاب الكراهية، انظر the United Nations Strategy and Plan of Action on Hate Speech (2019). يمكن الاطلاع عليه في الرابط التالي: www.un.org/en/genocideprevention/hate-speech-strategy.shtml.

(37) في القانون الجنائي، يمكن اعتبار الجناة مسؤولين استناداً إلى عدد من أنماط المسؤولية، على النحو المحدد في النظام الأساسي المعني. وتشمل أنماط المسؤولية هذه الارتكاب المباشر وغير المباشر والمشاركة في الارتكاب والمساعدة والتحريض ومسؤولية القيادة. انظر Jérôme de Hemptinne, Robert Roth and Elies van Sliedregt, eds., *Modes of Liability in criminal law* (Cambridge, United Kingdom, Cambridge University Press, 2019).

(38) انظر، على سبيل المثال، المحكمة الجنائية الدولية، القواعد الإجرائية وقواعد الإثبات (2013)؛ المحكمة الدولية ليوغوسلافيا السابقة، القواعد الإجرائية وقواعد الإثبات (8 تموز/يوليه 2015)؛ المحكمة الجنائية الدولية لرواندا، القواعد الإجرائية وقواعد الإثبات (13 أيار/مايو 2015)؛ محكمة سيراليون الخاصة لتصريف الأعمال المتبقية، القواعد الإجرائية وقواعد الإثبات (30 تشرين الثاني/نوفمبر 2018)؛ المحكمة الخاصة بلبنان، القواعد الإجرائية وقواعد الإثبات (10 نيسان/أبريل 2019)؛ الدوائر الاستثنائية في محاكم كمبوديا، القواعد الداخلية (3 آب/أغسطس 2011).

(39) على سبيل المثال، كُلفت البعثة الدولية المستقلة لتقصي الحقائق بشأن جمهورية فنزويلا البوليفارية، التي أنشئت في أيلول/سبتمبر 2019، بالتحقيق في حالات الإعدام خارج نطاق القضاء والاختفاء القسري والاحتجاز التعسفي والتعذيب وغيره من ضروب المعاملة القاسية أو اللاإنسانية أو المهينة منذ عام 2014 وتقديم تقرير عن النتائج التي توصلت إليها إلى المجلس (قرار مجلس حقوق الإنسان 25/42، الفقرة 24). وكُلفت لجنة التحقيق الدولية المستقلة المعنية بالجمهورية العربية السورية، التي أنشئت في عام 2011، بالتحقيق في جميع انتهاكات القانون الدولي لحقوق الإنسان المزعومة منذ آذار/مارس 2011 في الجمهورية العربية السورية وتحديد الوقائع والظروف التي قد ترقى إلى مستوى هذه الانتهاكات والجرائم المرتكبة، وحيثما أمكن، تحديد المسؤولين عنها (قرار مجلس حقوق الإنسان د إ-1/17، الفقرة 13). وكُلِّف فريق الخبراء الدولي الذي أرسل إلى منطقة كاساي في جمهورية الكونغو الديمقراطية في عام 2017 بجمع المعلومات المتعلقة بانتهاكات وتجاوزات حقوق الإنسان المزعومة وحفظها، وانتهاكات القانون الدولي الإنساني في مناطق كاساي وإحالة استنتاجات هذا التحقيق إلى السلطات القضائية في جمهورية الكونغو الديمقراطية (قرار مجلس حقوق الإنسان 33/35، الفقرة 10).

(40) كثيراً ما يكون لبعض المنظمات، ومن بينها منظمات غير حكومية، منهجياتها الداخلية التي تتطلب منها التركيز على مجال معين من مجالات القانون، على سبيل المثال فيما يتعلق بالتعذيب أو العنف الجنسي والعنف الجنساني التي تتيح أيضاً إرشادات بشأن مجال التركيز في التحقيقات.

والفئات الثلاث هذه يعزز بعضها بعضاً؛ فانطباق القانون الدولي الإنساني و/أو القانون الجنائي الدولي لا يعفي الدول من الوفاء بالتزاماتها بموجب القانون الدولي لحقوق الإنسان. وفيما يلي لمحة عامة عن كل مجال من مجالات الممارسة، بما في ذلك مصادر القانون والفروق بين مجالات الممارسة، حتى يتسنى للمحققين المتخصصين في المصادر المفتوحة معرفة المراجع التي ينبغي أن توجه عملهم.

1- القانون الدولي الإنساني

43- ينظِّم القانون الدولي الإنسان أو "قانون النزاعات المسلحة" سير الأعمال العدائية ويحل القضايا الإنسانية التي تنشأ في سياق هذه النزاعات وقد تكون ذات طبيعة دولية أو غير دولية[41]. ويتم تفعيل القانون الدولي الإنساني عندما يندلع نزاع مسلح ويمتد نطاق هذا القانون إلى أن يتحقق السلام، وإن لم تكن هذه المسارات محددة أو مباشرة على الـدوام[42]. والمصادر الرئيسية للقانون الدولي الإنساني هي اتفاقيتا لاهاي لعامي 1899 و1907[43] واتفاقيات جنيف المؤرخة 12 آب/أغسطس 1949[44] والبروتوكولان الإضافيان الملحقان بها لعام 1977[45]، فضلاً عن عدة معاهدات تنظم استخدام أنواع معينة من الأسلحة[46]. ويشكِّل القانون العرفي أيضاً مصدراً هاماً للقانون الدولي الإنساني لأنه يسد الثغرات التي تخلفها المعاهدات. والقانون الدولي الإنساني العرفي ملزم لجميع أطراف النزاع وهو يكتسي أهمية خاصة في النزاعات المسلحة غير الدولية فقواعده في هذا الشأن أكثر تفصيلاً من قواعد القانون الدولي الإنساني القائم على المعاهدات[47]. وحتى مطلع التسعينات، كانت المحاكم العسكرية الوطنية تمثل آليات إنفاذ القانون الدولي الإنساني الأساسية حيث تقوم الدول بمساءلة أفرادها وضباطها المجندين. ومع ظهور المحاكم الجنائية الدولية، تم تدوين بعض انتهاكات القانون الدولي الإنساني ضمن النظام

(41) يستند التمييز بين النزاع المسلح الدولي وغير الدولي إلى عاملين هما: هيكل الأطراف المعنية ووضعها. وتشمل الصراعات المسلحة الدولية دولاً ذات سيادة. وعلى النقيض من ذلك، لا تشمل النزاعات المسلحة غير الدولية دولاً وجماعات مسلحة منظمة. انظر Andrew Clapham, Paola Gaeta and Marco Sassòli, eds., *The 1949 Geneva Conventions, A Commentary* (Oxford, Oxford University Press, 2015), chaps. 1 and 19.

(42) لئن كانت بداية الصراع الدولي واضحة نسبياً لأنها ناجمة عن أي استخدام للقوة بين دولتين، فإنَّ بدء نزاع مسلح غير دولي أقل وضوحاً. ولا تحدث النزاعات المسلحة غير الدولية إلا إذا كانت الجماعات المسلحة منظمة تنظيماً كافياً وبلغ مستوى العنف درجة معينة من الحدة – وهما عاملان يتطلبان تحليلاً وقائعياً مفصلاً على أساس كل حالة على حدة. انظر: Sylvain Vité, "Typology of armed conflicts in international humanitarian law: legal concepts and actual situations", International Review. of the Red Cross, vol. 91, No. 873 (March 2009), pp. 72 and 76-77. وهناك أيضاً خلاف بشأن موعد انتهاء النزاع المسلح وتحقيق السلام. ومع أنَّ اتفاقات وقف إطلاق النار أو السلام قد تساعد في إثبات نهاية الصراع المسلح، فإنها ليست إلزامية. واقتُرحت اختبارات مختلفة لنهاية نزاع مسلح، وهي الإيقاف العام للعمليات العسكرية عند التوصل إلى اتفاق عام للسلام ووجود تسوية سلمية وانتفاء المعايير التي تحدد وجود النزاع. انظر Nathalie Weizmann, "The end of armed conflict, the end of participation in armed conflict, and the end of hostilities: implications for the detention operations under the 2001 AUMF", *Columbia Human Rights Law Review*, vol. 47, No. 3(2016), pp. 221-224.

(43) على التوالي، الاتفاقية المتعلقة بقوانين وأعراف الحرب البرية (اتفاقية لاهاي الثانية) والاتفاقية المتعلقة بقوانين وأعراف الحرب البرية (اتفاقية لاهاي الرابعة).

(44) انظر اتفاقية جنيف لتحسين حالة الجرحى والمرضى بالقوات المسلحة في الميدان (اتفاقية جنيف الأولى)؛ اتفاقية جنيف لتحسين حال جرحى ومرضى وغرقى القوات المسلحة في البحار (اتفاقية جنيف الثانية)؛ اتفاقية جنيف المتعلقة بمعاملة أسرى الحرب (اتفاقية جنيف الثالثة)؛ اتفاقية جنيف بشأن حماية الأشخاص المدنيين في وقت الحرب (اتفاقية جنيف الرابعة).

(45) انظر البروتوكول الإضافي الملحق باتفاقيات جنيف المعقودة في 12 آب/أغسطس 1949 والمتعلق بحماية ضحايا المنازعات المسلحة الدولية لعام 1949 (البروتوكول الأول)؛ البروتوكول الإضافي لاتفاقيات جنيف المعقودة في 12 آب/أغسطس 1949، والمتعلق بحماية ضحايا المنازعات المسلحة غير الدولية (البروتوكول الثاني).

(46) انظر، على سبيل المثال، اتفاقية حظر استحداث وإنتاج وتخزين الأسلحة البكتريولوجية (البيولوجية) والتكسينية وتدمير تلك الأسلحة؛ اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر؛ اتفاقية حظر استحداث وإنتاج وتخزين واستعمال الأسلحة الكيميائية وتدمير تلك الأسلحة؛ اتفاقية حظر استعمال وتخزين وإنتاج ونقل الألغام المضادة للأفراد، وتدمير تلك الألغام؛ اتفاقية بشأن الذخائر العنقودية. انظر أيضاً International Committee of the Red Cross (ICRC), "Weapons", 30 November 2011. يمكن الاطلاع عليه في الرابط التالي: www.icrc.org/ar/document/weapons.

(47) انظر ICRC, "Customary international humanitarian law", 29 October 2010. يمكن الاطلاع عليه في الرابط التالي: www.icrc.org/Ar/document/customary-international-humanitarian-law-0. انظر أيضاً ICRC, "Welcome to the Customary IHL Database". يمكن الاطلاع عليه في الرابط التالي: https://ihl-databases.icrc.org/ar/customary-ihl.

الأساسي التأسيسي للمحاكم بحسبانها جرائم حرب[48]، فأُتيح سبيل جديد لإنفاذ القانون الدولي الإنساني على الصعيد الدولي. ودونت بعض الدول أيضاً جرائم الحرب في تشريعاتها الوطنية[49]، بحيث يمكن النظر في هذه القضايا في إطار نظمها القضائية العادية، بدلاً من المحاكم العسكرية. وقد تُثار قضايا وطنية في بلد النزاع أو بصورة متزايدة في بلدان أخرى بموجب مبدأ الولاية القضائية العالمية[50]. وقد أنشأ عدد من الدول وحدات متخصصة في جرائم الحرب للتحقيق في هذه القضايا. وتسهم المحاكم الجنائية الدولية والمحاكم الوطنية في ازدياد مجموعة الاجتهادات المتعلقة بالقانون الدولي الإنساني التي تشكل أيضاً مصدراً هاماً للقانون وقد تكون أحكامها ملزمة تبعاً للولاية القضائية.

2- القانون الدولي لحقوق الإنسان

44- تقع على عاتق الدول التزامات وواجبات بموجب القانون الدولي باحترام حقوق الإنسان وحمايتها وإعمالها. ويرسي الإعلان العالمي لحقوق الإنسان الذي اعتمد في عام 1948 الأساس للقانون الدولي لحقوق الإنسان. ومع أنَّ هذا الإعلان تطلعي وغير ملزم قانوناً، فإنَّ بعض مواده تشكل جزءاً من القانون الدولي العرفي[51]، فضلاً عن أنَّه كان مصدر إلهام لعهدين ولمجموعة ثرية من معاهدات حقوق الإنسان[52]. ولا تلتزم الدول إلا بالعهود والمعاهدات التي وقعتها وصدقت عليها، ما لم تكن المعايير الواردة في تلك الوثائق قد اكتسبت وضع القانون الدولي العرفي[53]. وأُدمج القانون الدولي لحقوق الإنسان أيضاً في الإطار القانوني للعديد من المحاكم الجنائية الدولية. وبالإضافة إلى ذلك، توجد محاكم إقليمية عديدة لحقوق الإنسان منشأة بموجب الاتفاقيات الدولية أُسندت إليها ولايات للفصل في القضايا المرفوعة ضد الدول الأطراف في تلك الاتفاقيات بسبب انتهاكات القانون الدولي لحقوق الإنسان، بما في ذلك المحكمة الأفريقية لحقوق الإنسان والشعوب[54]، والمحكمة الأوروبية لحقوق الإنسان[55] ومحكمة البلدان الأمريكية لحقوق الإنسان[56]. وتوجد هيئات إضافية لحقوق الإنسان على الصعيد الإقليمي، من بينها اللجنة الأفريقية لحقوق الإنسان والشعوب واللجنة الأوروبية للحقوق الاجتماعية ولجنة البلدان الأمريكية لحقوق الإنسان، وكلها تواصل تطوير الاجتهادات المتعلقة بالقانون الدولي لحقوق الإنسان.

(48) على سبيل المثال، تدون المادة 8 من نظام روما الأساسي للمحكمة الجنائية الدولية القانون الدولي الإنساني في تعريفها لجرائم الحرب.

(49) انظر على سبيل المثال، Australia (War Crimes Act 1945, as amended, sect. 7); Bosnia and Herzegovina (Criminal Code, arts. 171-184); Kenya (International Crimes Act 2008, sect. 6(1)(c) and (2)-(4)); New Zealand (International Crimes and International Criminal Court Act 2000, sect. 11); South Africa (Implementation of the Geneva Conventions Act 2012).

(50) بموجب "الولاية القضائية العالمية"، يجوز للمحكمة الوطنية مقاضاة الأفراد على الجرائم الخطيرة المرتكبة ضد القانون الدولي – مثل الجرائم ضد الإنسانية وجرائم الحرب والإبادة الجماعية والتعذيب – التي تقع خارج حدود الدولة، استناداً إلى المبدأ القائل بأنَّ هذه الجرائم تضر بالمجتمع الدولي والنظام الدولي نفسه اللذين يجوز لفرادى الدول اتخاذ إجراءات لحمايتهما. انظر International Justice Resource Center, "Universal jurisdiction". يمكن الاطلاع عليه على الرابط التالي: https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

(51) ذكر العديد من البلدان ومن مسؤولي الأمم المتحدة والعلماء أنَّ غالبية المواد الواردة في الإعلان العالمي لحقوق الإنسان، إن لم تكن جميعها، تشكل قانوناً دولياً عرفياً. وعلى وجه التحديد، فإن حظر الرق والحرمان التعسفي من الحياة والتعذيب والاحتجاز التعسفي والتمييز العنصري المدون في الإعلان العالمي لحقوق الإنسان مقبول بحسبانه يشكل القانون الدولي العرفي. انظر Hurst Hannum, "The status of the Universal Declaration of Human Rights in national and international law", *Georgia Journal of International and Comparative Law*, vol. 25, No. 1(1996), pp. 322-332 and 341-346.

(52) انظر الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري؛ العهد الدولي الخاص بالحقوق المدنية والسياسية؛ العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية؛ اتفاقية القضاء على جميع أشكال التمييز ضد المرأة؛ اتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة؛ اتفاقية حقوق الطفل. وللاطلاع على مزيد من المعلومات عن معاهدات الأمم المتحدة الأساسية لحقوق الإنسان، انظر OHCHR, "The core international human rights instruments and their monitoring". يمكن الاطلاع عليه على الرابط التالي: www.ohchr.org/en/ProfessionalInterest/Pages/CoreInstruments.aspx.

(53) يشير القانون الدولي العرفي إلى الالتزامات الدولية الناشئة عن الممارسات الدولية الراسخة في مقابل الالتزامات الناشئة عن الاتفاقيات والمعاهدات المكتوبة الرسمية. وهو ينشأ عن ممارسة عامة ومتسقة للدول تتبعها من منطلق الالتزام القانوني. ومن العناصر الأساسية للقانون الدولي العرفي القواعد الآمرة التي تشير إلى بعض مبادئ القانون الدولي الأساسية والغالبة. انظر، على سبيل المثال، Legal Information Institute, "Customary international law" and "Jus cogens", Cornell Law School. يمكن الاطلاع عليه على الرابط التالي: www.law.cornell.edu/wex.

(54) أنشئت عملاً بالميثاق الأفريقي لحقوق الإنسان والشعوب (ميثاق بانجول).

(55) أنشئت عملاً باتفاقية حماية حقوق الإنسان والحريات الأساسية (الاتفاقية الأوروبية لحقوق الإنسان).

(56) أنشئت عملاً بالاتفاقية الأمريكية لحقوق الإنسان (ميثاق سان خوسيه).

45- وتؤدي المنظمات الدولية أيضاً دوراً رئيسياً في وضع القانون الدولي العرفي لحقوق الإنسان وإنشاء معاييره[57]. وتصدر مفوضية الأمم المتحدة لحقوق الإنسان وهيئات دولية أخرى تقارير مواضيعية بشأن مجالات قانونية تسهم في وضع المعايير والقوانين غير الملزمة. أما هيئات معاهدات حقوق الإنسان[58] فتتولى إصدار تقارير[59]، واجتهادات[60] وأنواع أخرى من الإرشادات، بما فيها التعليقات العامة والتوصيات العامة[61] التي تسهم في تطوير مواد معاهدات كل منها وفي فهمها. وبالمثل، تؤدي الإجراءات الخاصة لمجلس حقوق الإنسان دوراً في تطوير معايير في القانون الدولي لحقوق الإنسان[62]، شأنها في ذلك شأن الآليات الأخرى، ومن بينها بعثات تقصي الحقائق ولجان التحقيق.

46- وعلى غرار القانون الدولي الإنساني، أصبح القانون الدولي لحقوق الإنسان جزءاً من الإطار القانوني للعديد من البلدان، إما نتيجة للتقاليد القانونية الأحادية التي تطبق الالتزامات الدولية مباشرة في المجال الوطني أو من خلال الإدماج المباشر للقانون الدولي في التشريعات الوطنية أو بتطبيق الولاية القضائية العالمية، على نحو يؤدي إلى تطوير اجتهادات هامة بشأن هذا القانون[63].

3- القانون الجنائي الدولي

47- ينطبق القانون الجنائي الدولي في أوقات السلم وأثناء النزاع المسلح على السواء ويفرض المسؤولية الجنائية على الأفراد الذين يرتكبون جرائم بموجب القانون الدولي، بما في ذلك جرائم الحرب والجرائم ضد الإنسانية والإبادة الجماعية[64].

(57) من أمثلة المنظمات الدولية المحكمة الجنائية الدولية والمنظمة الدولية للهجرة ومنظمة حظر الأسلحة الكيميائية، فضلاً عن آليات حقوق الإنسان، مثل الإجراءات الخاصة ولجان التحقيق التابعة لمجلس حقوق الإنسان أو ما يعادلها. وتمارس الإجراءات الخاصة ولاياتها فيما يتعلق بجميع الدول الأعضاء في الأمم المتحدة؛ فهي لا تعتمد على التصديق على معاهدة معينة. وتوجد اختلافات في القواعد القانونية وآلية آليات حقوق الإنسان هذه، فضلاً عن اختلافات في أساليب ومعايير جمع المعلومات. فعلى سبيل المثال، تتمثل طريقة العمل الرئيسية للفريق العامل المعني بالاحتجاز التعسفي في تلقي المعلومات من الأفراد المعنيين وأسرهم أو ممثليهم والحكومات والمنظمات غير الحكومية والمؤسسات الوطنية بشأن الحالات الفردية. ثم يحقق الفريق العامل في الحالات المبلغ عنها في البلاغات بوسائل من بينها الزيارات القطرية. انظر A/HRC/36/38 للاطلاع على أحدث أساليب عمل الفريق العامل. وعلى النقيض من ذلك، ينشئ مجلس حقوق الإنسان لجان التحقيق على أساس مخصص وهي عادة ما تشرع في تحقيقاتها الخاصة وفقاً لأحكام ولاياتها، وغالباً ما يتم ذلك من خلال زيارات قطرية تجري خلالها، من بين ما تجريه، مقابلات مع الشهود. انظر، على سبيل المثال، اختصاصات لجنة التحقيق المعنية ببوروندي. يمكن الاطلاع عليه على الرابط التالي: www.ohchr.org/Documents/HRBodies/HRCouncil/CoIBurundi/TermsofreferenceCOIBurundiENGL.pdf.

(58) انظر، على سبيل المثال، "OHCHR, Human rights treaty bodies". يمكن الاطلاع عليه على الرابط التالي: www.ohchr.org/ar/treaty-bodies/videos-about-treaty-bodies.

(59) يجوز أن تتخذ التقارير شكل ملاحظات ختامية تنظر بموجبها هيئة منشأة بموجب معاهدة في التقارير المقدمة من الدول الأطراف وغيرها من أصحاب المصلحة فيما يتعلق بتنفيذ التزامات الدول بموجب معاهدة معينة. وتستطيع بعض الهيئات المنشأة بموجب معاهدات أيضاً إصدار تقارير عن التحقيقات. انظر، على سبيل المثال، "Committee on the Elimination of Discrimination against Women, "Inquiry procedure". يمكن الاطلاع عليه على الرابط التالي www.ohchr.org/ar/treaty-bodies/cedaw/inquiry-procedure.

(60) تصدر الهيئات المنشأة بموجب معاهدات آراء بشأن الشكاوى الفردية استجابة لحالات معينة. انظر، بصفة عامة، مفوضية الأمم المتحدة السامية لحقوق الإنسان، "الهيئات المنشأة بموجب معاهدات حقوق الإنسان – البلاغات الفردية". متاح على الرابط التالي: www.ohchr.org/ar/treaty-bodies/human-rights-treaty-bodies-individual-communications.

(61) انظر مفوضية الأمم المتحدة السامية لحقوق الإنسان، "الهيئات المنشأة بموجب معاهدات حقوق الإنسان – تعليقات عامة". متاح على الرابط التالي: www.ohchr.org/ar/treaty-bodies/human-rights-treaty-bodies-general-comments.

(62) انظر، بصفة عامة، OHCHR, "Human rights treaty bodies - individual communications". يمكن الاطلاع عليه على الرابط التالي: www.ohchr.org/ar/special-procedures-human-rights-council.

(63) منظمة العفو الدولية، *Universal Jurisdiction: A Preliminary Survey of Legislation Around the World - 2012 Update* (London, 2012), pp. 1-2.

(64) Robert Cryer, Darryl Robinson and Sergey Vasiliev, *An Introduction to International Criminal Law and Procedure*, 4th ed. (Cambridge, United Kingdom, Cambridge University Press, 2019), chap. 15.

ويُشار إلى هذه الجرائم مجتمعة في بعض الأحيان بتعبير "الجرائم الوحشية" أو "الجرائم الدولية الخطيرة"[65]. وقد دونت هذه الجرائم بشكل كبير في نظام روما الأساسي الذي يعد على نطاق واسع تعبيراً عن القانون الجنائي الدولي العرفي. ويشمل القانون الجنائي الدولي أيضاً بعض الجرائم غير المدونة في نظام روما الأساسي، مثل الإرهاب[66]. وقد يكون هناك قدر من التداخل بين القانون الجنائي الدولي والمجال المعني في القانون الجنائي العابر للقوميات الذي يجرم الأفعال العابرة للحدود مثل الاتجار بالبشر والمخدرات والأسلحة وسواها من البضائع غير المشروعة[67]. وخلافاً للقانون الدولي الإنساني، والقانون الدولي لحقوق الإنسان، ينصب تركيز القانون الجنائي الدولي على المساءلة الجنائية الفردية بدلاً من مسؤولية الدول. ويمكن النظر في قضايا القانون الجنائي الدولي في المحاكم الجنائية الوطنية، أو المحاكم الجنائية المختلطة[68]، أو المحاكم الجنائية الدولية[69]، بما في ذلك المحكمة الجنائية الدولية، أو المحاكم المحلية التي تمارس الولاية القضائية العالمية. وتشمل مصادر القانون الجنائي الدولي الوثائق التأسيسية للمحاكم والهيئات القضائية (مثل قرارات مجلس الأمن والنظم الأساسية والقواعد الإجرائية وقواعد الإثبات والأنظمة الأساسية للمحاكم) والتشريعات الوطنية للدول التي تمارس ولايات قضائية على الجرائم الدولية. وثمة مصدر هام آخر للقانون الجنائي الدولي هو الاجتهادات، التي يمكن أن تكون ملزمة أو غير ملزمة حسب الولاية القضائية[70].

باء- الاختصاص القضائي والمساءلة

48- الاختصاص القضائي مصطلح قانوني يشير إلى السلطة الممنوحة لكيان قانوني، مثل محكمة أو هيئة قضائية، لسن قانون والبت فيه وإنفاذه. ويعرف البروتوكول العدالة والمساءلة تعريفاً واسعاً للإشارة إلى أنواع مختلفة من العمليات القضائية وغير القضائية. وقد تنجم المساءلة عن الجرائم الدولية وانتهاكات القانون الدولي لحقوق الإنسان و/أو القانون الدولي الإنساني عن إجراءات قانونية قد تكون جنائية أو مدنية أو إدارية بطبيعتها وكذلك عن عمليات غير ملزمة قانوناً، مثل تقارير التحقيقات الدولية في مجال حقوق الإنسان، بما في ذلك لجان التحقيق وبعثات تقصي الحقائق، وغيرها من آليات العدالة الانتقالية، مثل المبادرات التي تركز على البحث عن الحقيقة. وينبغي للمحققين أن يسعوا، حيثما أمكن ذلك، إلى مراعاة نطاق الولايات القضائية الممكنة التي يمكن السعي إلى المساءلة فيها.

49- وينبغي للمحققين المتخصصين في المصادر المفتوحة أن يحددوا آليات المساءلة ذات الصلة بعملهم والأماكن المحتملة التي يمكن أو قد تُقبل فيها الأدلة التي جُمعت لإثبات الحقائق. ومع ذلك، في المراحل المبكرة من التحقيقات الدولية قد تكون تلك الآليات غير معروفة أو غير واضحة. ويصدق هذا بصفة خاصة حين لا يكون لدى الدولة التي ارتُكبت فيها الجرائم نظام قضائي فعال، أو عندما لا تكون القضية قد عُرضت بالكامل على المجتمع الدولي بغية التحقيق في الأمر. وعلاوة على ذلك، قد يتعذر التنبؤ بجميع الولايات القضائية ذات الصلة في المستقبل. وعندما يجهل المحققون المتخصصون في المصادر المفتوحة الآلية أو الولاية القضائية المعنية، ينبغي عليهم أن يسعوا جاهدين لجمع المعلومات والحفاظ عليها بطريقة تزيد من استخدامها في أوسع نطاق من الولايات القضائية التي يمكن أن تكون ذات صلة. وإن كان المحققون على علم بالمتطلبات المتعلقة بالمكان الذي ستقدم فيه القضية للمحاكمة في نهاية المطاف، فيجدر بهم تكييف عملياتهم مع تلك المتطلبات المحددة.

50- ويمكن إنشاء الاختصاص القضائي بالطرق التالية:

(أ) الولاية القضائية الإقليمية هي السلطة التي تخول المحكمة النظر في قضايا متعلقة بأفعال تقع في إقليم

(65) على الرغم من أن مصطلح "التطهير العرقي" غير مدرج في نظام روما الأساسي، ولا يعرف بأنه جريمة مستقلة بموجب القانون الدولي، فقد اعتبر أنه ينتمي إلى فئة "الجرائم الفظيعة". وفي هذا السياق، انظر United Nations, "Framework of analysis for atrocity crimes: a tool for prevention", p. 1. يمكن الاطلاع عليه على الرابط التالي: www.un.org/en/genocideprevention/documents/about-us/Doc.3_Framework%20of%20Analysis%20for%20Atrocity%20Crimes_EN.pdf.

(66) انظر قرار مجلس الأمن 1757(2007)، المرفق، الضميمة (النظام الأساسي للمحكمة الخاصة بلبنان)، المادة 2.

(67) Cryer, Robinson and Vasiliev, *An Introduction to International Criminal Law and Procedure*, chap. 15.

(68) يشمل هذا المصطلح، في جملة أمور، الدوائر الاستثنائية في محاكم كمبوديا والمحكمة الخاصة لسيراليون والمحكمة الخاصة بلبنان والدوائر المتخصصة لكوسوفو ومكتب المدعي العام والمحكمة الجنائية الخاصة لجمهورية أفريقيا الوسطى.

(69) يشمل هذا المصطلح المحكمة الجنائية الدولية الدائمة والمحكمة الدولية المخصصة ليوغوسلافيا السابقة والمحكمة الجنائية الدولية لرواندا والآليّة الدولية لتصريف الأعمال المتبقية للمحكمتين الجنائيتين الدوليتين.

(70) انظر Rosa Theofanis, "The doctrine of res judicata in international criminal law", *International Criminal Law Review*, vol. 3, No. 3(2003).

محدد. وفي حالة المحاكم الدولية، يقتصر الاختصاص الإقليمي عادة على أراضي الدول التي صدَّقت على المعاهدة التأسيسية؛

(ب) الاختصاص الزمني هو السلطة التي تخول المحكمة النظر في قضايا وقعت فيها أفعال مدعى ارتكابها خلال فترة زمنية محددة؛

(ج) الاختصاص الشخصي هو السلطة التي تخول المحكمة اتخاذ القرارات المتعلقة بطرف في الدعوى؛

(د) الاختصاص الموضوعي هو السلطة التي تخول للمحكمة النظر في قضايا من نوع معين، أو في قضايا تتعلق بموضوع معين؛

(هـ) الولاية القضائية العالمية هي ادعاء المحكمة بسلطة على شخص متهم بغض النظر عن مكان ارتكاب الجريمة المزعومة وعن جنسية المتهم، أو بلد إقامته، أو أي علاقة أخرى مع الجهة التي تقوم بالمقاضاة.

جيم- سلطات وواجبات التحقيق

51- سلطات التحقيق الرسمية هي تلك التي يخولها القانون لكيان معين للتحقيق داخل ولاية قضائية معينة. وعلى غرار القيود المفروضة على السلطة القضائية إلى حد كبير، لا يجوز لأي هيئة قضائية، أو هيئة ادعاء، إجراء تحقيقات إلا بقدر ما يسمح به القانون[71]. وتشمل سلطات التحقيق القدرة على إجبار الشهود وسجلات الاستدعاء وتنفيذ مذكرات التفتيش. وقد يقتضي القانون من هيئة التحقيق أن تتبع إجراءات صارمة، أو قد يسمح لها، في بعض الحالات، بتحديد إجراءاتها الخاصة[72].

52- ولا تخول عموماً لمعظم الهيئات الأخرى التي تحقق في انتهاكات القانون الدولي سلطات التحقيق أو الوسائل القابلة للإنفاذ لجمع الأدلة، مثل مذكرات الاستدعاء أو أوامر التفتيش. وبالتالي، فقد تعتمد هذه الهيئات اعتماداً كلياً على المعلومات المفتوحة المصدر والمعلومات المقدمة طوعاً، مثل الوثائق والملفات الرقمية وشهادات الشهود.

53- وعموماً، تقترن سلطات التحقيق بواجبات محددة[73]. ورغم أنَّ بعض المحققين قد لا يتمتعون بسلطات الشرطة أو بسلطات هيئة قانونية أخرى، يوصى، قدر المستطاع، بأن يسعى جميع المحققين إلى الالتزام بواجباتهم القانونية الرئيسية، حرصاً عل جودة التحقيقات. وتشمل واجبات والتزامات المحققين القانونيين والمدعين العامين المشتركة واجب التحقيق في ظروف التجريم والتبرئة وواجب حماية الشهود والحفاظ على الأدلة وضمان عدالة الإجراءات والالتزام باحترام حقوق المتهمين.

54- وفي المحاكمات الجنائية، يلزم المدعون العامون أيضاً بالكشف للدفاع عن المعلومات والأدلة ذات الصلة[74]. ولا يقتصر ذلك على الأدلة التي تُقبل في المحاكمة فحسب، بل ويشمل أي معلومات تُجمع في إطار تحقيق يجِّرم أو يبُرئ، ويتضمن ذلك المعلومات عن مصداقية الشهود[75]. وتوجد بعض الاستثناءات المتعلقة بالمعلومات المميزة أو المعلومات التي قد تعرِّض الشخص للخطر. ويجوز للمحكمة أن تأمر بعدم الكشف عن هوية الضحية أو الشاهد الذي قد يتعرض للخطر بسبب هذا الكشف، بيد أنَّ ذلك لا يكون أكيداً قط[76]. ولدى العديد

(71) انظر Justia, "Agency investigations". يمكن الاطلاع عليه على الرابط التالي: www.justia.com/administrative-law/agency-investigations.

(72) المرجع نفسه.

(73) على سبيل المثال، تحدد المادة 54 من نظام روما الأساسي واجبات المدعي العام وسلطاته فيما يتعلق بالتحقيقات، وتنشئ قدرة المدعي العام، في جملة أمور، على إجراء التحقيقات وجمع الأدلة وفحصها ومقابلة الضحايا والشهود والتعاون مع الدول والمنظمات الدولية.

(74) انظر، على سبيل المثال، المحكمة الدولية ليوغوسلافيا السابقة، القواعد الإجرائية وقواعد الإثبات، القاعدة 66(ألف)؛ المحكمة الجنائية الدولية لرواندا، القواعد الإجرائية وقواعد الإثبات، القاعدة 66(ألف)؛ المحكمة الخاصة بلبنان، القواعد الإجرائية وقواعد الإثبات، القاعدة 110(ألف).

(75) انظر، على سبيل المثال، المحكمة الجنائية الدولية، القواعد الإجرائية وقواعد الإثبات، القواعد 76–84؛ المحكمة الدولية ليوغوسلافيا السابقة، القواعد الإجرائية وقواعد الإثبات، القاعدة 66(ألف)'2'؛ المحكمة الجنائية الدولية لرواندا، القواعد الإجرائية وقواعد الإثبات، القاعدة 66(أ)'2'؛ المحكمة الخاصة لسيراليون، القواعد الإجرائية وقواعد الإثبات، القاعدة 66(ألف)'2'؛ المحكمة الخاصة بلبنان، القواعد الإجرائية وقواعد الإثبات، القاعدة 110(ألف)'2'؛ الأفرقة الخاصة المعنية بالجرائم الخطيرة في تيمور – ليشتي، القواعد الانتقالية للإجراءات الجنائية، الفرع 24–4.

(76) انظر، على سبيل المثال، المحكمة الجنائية الدولية، القواعد الإجرائية وقواعد الإثبات، القاعدة 81(4)؛ المحكمة الدولية ليوغوسلافيا السابقة، القواعد الإجرائية وقواعد الإثبات، القاعدة 69؛ المحكمة الجنائية الدولية لرواندا، القواعد الإجرائية وقواعد الإثبات، القاعدة 69؛ المحكمة الخاصة لسيراليون، القواعد الإجرائية وقواعد الإثبات، القاعدة 69؛ المحكمة الخاصة بلبنان، القواعد الإجرائية وقواعد الإثبات، القاعدتان 115–116؛ الأفرقة الخاصة المعنية بالجرائم الخطيرة في تيمور – ليشتي، القواعد الانتقالية للإجراءات الجنائية، الفرع 24–6.

من الولايات القضائية الجنائية قواعد للكشف تقتضي من المدعين العامين تسليم أي شيء من شأنه أن يكون مبرئاً[77]. وينبغي للمحققين المتخصصين في المصادر المفتوحة الذين يعملون في أي قضية توجد أدنى فرصة بأن ينتهي بها المطاف في المحكمة أن يأخذوا التزامات الكشف هذه في الحسبان عند الاضطلاع بعملهم[78]. وثمة أسباب أخرى عديدة تجعل المحققين ينظرون في إمكانية الكشف عن المعلومات. فعلى سبيل المثال، إذا طلب من المدعين العامين مراجعة جميع المواد التي جُمعت في التحقيق، فينبغي عليهم تجنب جمع المعلومات بكميات كبيرة، لأن حجم المعلومات الكبير قد يشكل عبئاً ثقيلاً، بل وقد تستحيل مراجعته. ولهذا الأمر أهميته أيضاً في حفظ المعلومات التي جُمعت وتخزينها، بما في ذلك التوسيم المناسب، مما يعود بفائدة كبيرة على الساعين إلى استرداد المواد ومراجعتها لاحقاً.

دال– القواعد الإجرائية وقواعد الإثبات

55– عند العمل في سياق تحقيق قانوني، تتمثل مهمة المحققين المتخصصين في المصادر المفتوحة الرئيسية في جمع المعلومات ذات الصلة والمعلومات الأصلية لاستخدامها في استخلاص استنتاجات واقعية وقانونية. ويجب على المحققين، ولا سيما في المحاكم والهيئات القضائية الدولية، أن يسعوا إلى التحقق من أن تكون أي أدلة مفتوحة المصدر تُجمع مقبولة وذات صلة بالموضوع وموثوق بها وإثباتية. وتتميز التحقيقات الجنائية عن التحقيقات التي تجرى لأغراض أخرى بمستوى الإثبات المرتفع المنطبق عليها[79] وبقواعد إجرائية وقواعد إثبات أكثر صرامة، تشمل المقبولية، حرصاً على حماية الإجراءات وفق الأصول القانونية وصوناً لحقوق أي أشخاص متهمين في محاكمة عادلة[80]. ورغم أنّ الحد الأدنى الذي يحول دون مقبولية الأدلة في المحاكم الجنائية الدولية والهيئات القضائية الدولية عادة ما يكون أقل من نظيره المعمول به في بعض المحاكم الوطنية، فإنَّ أساليب جمع الأدلة ستؤثر مع ذلك على الوزن الذي يقيمه القضاة للأدلة. وينطبق ذلك في جميع الولايات القضائية. وفي عصر سمته انتشار المعلومات الرقمية، ومن بينها المعلومات المغلوطة والمضللة على حد سواء[81]، فإنَّ من الأهمية بمكان أن يتمكن المحققون من التثبت من أن تكون المعلومات المفتوحة المصدر أصلية ومن إثبات صحتها، أو دحضها، بدقة كافية[82].

56– وفي الإجراءات القضائية، تشير المقبولية إلى المدى الذي يجوز فيه قبول عنصر يقدمه طرف في الإجراءات في سجل القضية كدليل. وبوجه عام، تُقيِّم المحاكم الجنائية الدولية مقبولية العنصر المعروض عليها باستخدام اختبار

(77) انظر على سبيل المثال المحكمة الدولية ليوغوسلافيا السابقة، القواعد الإجرائية وقواعد الإثبات، القاعدة 68؛ المحكمة الجنائية الدولية لرواندا، القواعد الإجرائية وقواعد الإثبات، القاعدة 68؛ المحكمة الخاصة لسيراليون، القواعد الإجرائية وقواعد الإثبات، القاعدة 68؛ المحكمة الخاصة بلبنان، القواعد الإجرائية وقواعد الإثبات، القاعدة 113؛ نظام روما الأساسي للمحكمة الجنائية الدولية، المادة 67(2)؛ الأفرقة الخاصة المعنية بالجرائم الخطيرة في تيمور الشرقية، القواعد الإجرائية وقواعد الإثبات، القاعدة 24–4(ج). أدلة البراءة هي الأدلة التي قد تبرئ المدعى عليه. وفي الولايات المتحدة، يمثل مبدأ برادي قاعدة اكتشاف قبل المحاكمة وضعتها المحكمة العليا للولايات المتحدة، وهي تشترط أن يسلم الادعاء جميع أدلة البراءة إلى المدعى عليه في قضية جنائية. انظر *Brady v. Maryland*, 378 U.S. 83(1963).

(78) نظراً لأنّ التزامات الكشف قد تتطلب تسليم بعض المواد المجمعة، أو كلها، إلى الدفاع، فقد تنتفي قدرة المحققين المتخصصين في المصادر المفتوحة على حماية الهويات وغيرها من المعلومات الحساسة.

(79) على سبيل المثال، تطبق المحاكم الدولية عادة معيار الإثبات في القانون الجنائي "بما لا يدع مجالا لِلشك المعقول"، بينما تعتمد لجان التحقيق والهيئات المماثلة لها عادة المعيار الأدنى من ذلك المتمثل في "وجود أسباب معقولة تدعو للاعتقاد" الذي تستند إليه في استنتاجاتها. وللاطلاع على مزيد من المعلومات، انظر OHCHR, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, pp. 62-63.

(80) المحكمة الجنائية الدولية، *المدعي العام ضد جان – بيير بيمبا*، القضية رقم ICC-01/05-01/08 A، الحكم الصادر في استئناف السيد جان بيير بيمبا غومبو ضد "الحكم الصادر عن الدائرة الابتدائية الثالثة عملاً بالمادة 74 من النظام الأساسي"، 8 حزيران/يونيه 2018، غرفة الاستئناف، رأي منفصل للقاضي فان دن فينغارت والقاضي موريسون، الفقرة 5.

(81) المعلومات المغلوطة هي معلومات كاذبة، ولكن لا يُقصد منها تسبيب ضرر. فعلى سبيل المثال، قد ينشر أفراد لا يعلمون أنَّ المعلومة كاذبة هذه المعلومة على وسائل التواصل الاجتماعي، ظناً منهم أنَّها ستكون مفيدة. والمعلومات المضللة هي معلومات كاذبة يتم اختلاقها أو نشرها عمداً لغرض صريح هو التسبب في ضرر. وعادة ما تكون دوافع مختلقي المعلومات المضللة سياسية أو مالية أو نفسية أو اجتماعية. انظر Claire Wardle, "Information disorder: the essential glossary", Cambridge, Massachusetts, Shorenstein Center on Media, Politics and Public Policy, 2018. يمكن الاطلاع عليه في الرابط التالي: https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x32994.

(82) المرجع نفسه.

يتألف من ثلاثة عوامل هي: (أ) الأهمية؛ (ب) القيمة الإثباتية؛ (ج) القيمة الإثباتية من منظور التأثير على عدالة المحاكمة[83]. ويكون العنصر ذا صلة إن ساعد في جعل حقيقة ما أكثر أو أقل احتمالاً، بينما تشير قيمته الإثباتية إلى مدى فائدته في إثبات حقيقة قيد النظر في القضية، أو في دحضها. وفي حالة التحقيقات غير القضائية، يطبق تقييم مماثل للمقبولية. وينبغي تقييم كل معلومة من حيث موثوقيتها وأهميتها وقيمتها الإثباتية لتقرير إن كان ينبغي استخدامها وسبل ذلك في تحديد الاستنتاجات القانونية و/أو الوقائعية[84].

57- ويشير الوزن إلى القيمة التي تُنسب إلى عنصر ما ودرجة الاعتماد عليه في نهاية المطاف في استخلاص استنتاج قانوني أو وقائعي. وينبغي أن يتمثل تحديد الوزن في تقييم شامل يعتمد، في شق منه، على المعلومات الأخرى التي تدعم الحقيقة المعنية، أو تؤيدها، أو تناقضها. وفي العديد من الإجراءات القانونية، تُقيَّم المقبولية والوزن بشكل منفصل. وفي سياقات أخرى، وفي الحالات التي لا تشكل فيها مقبولية الأدلة عاملاً، يطبق المحققون في مجال حقوق الإنسان نهجاً مماثلاً في تقييم الوزن الذي يُسند إلى المعلومات.

58- ويمكن الاطلاع على القواعد الإجرائية وقواعد الإثبات المنطبقة على الإجراءات الجنائية الدولية في الصكوك التأسيسية لكل محكمة، وعلى الأخص قواعدها الإجرائية وقواعدها للإثبات. وتتيح الاجتهادات مزيداً من الإرشادات. وحسب طبيعة التحقيق، قد يكون من المفيد الاتصال بخبير قانوني التماساً لمشورته. ويصدق هذا بصفة خاصة حين يكون الغرض من التحقيق المساهمة في إجراءات المحكمة.

59- وقد تتألف المعلومات المفتوحة المصدر من مزيج من الأدلة الوثائقية والأدلة المستمدة من الشهادات. فعلى سبيل المثال، يجب التثبت من صحة مقطع فيديو يظهر فيه شخص يدلي بشهادات والتحقق من البيانات المدلى بها في إطارها بشكل منفصل[85]. ولذلك، قد تنطبق وسائل توثيق العنصر الرقمي كمستند أو تقييم موثوقيته ومقبوليته كدليل على الشهادة. وينبغي أن يكون المحققون على دراية بالأساليب التي تُعامل بها كل فئة من فئات الأدلة في الولاية القضائية المعنية. ويمكن في كثير من الأحيان قبول الأدلة المستندية حتى وإن لم يكن صاحبها معروفاً أو متاحاً للإدلاء بشهادته. وقد تكون هذه الأدلة مقبولة أيضاً دون الاضطرار إلى تقديم المستند عن طريق شاهد بوسعه تأكيد صحته، شريطة أن يتمكن الطرف الذي يعرض المستند من أن يثبت

(83) بموجب نظام روما الأساسي (المادتان 64(9)(أ) و69(4))، يكون للدائرة الابتدائية للمحكمة الجنائية الدولية "سلطة القيام بناء على طلب أحد الأطراف أو من تلقاء نفسها ... الفصل في مقبولية الأدلة أو صلتها ... آخذة في اعتبارها جملة أمور، ومنها القيمة الإثباتية للأدلة وأي إخلال قد يترتب على هذه الأدلة فيما يتعلق بإقامة محاكمة عادلة للمتهم أو بالتقييم المنصف لشهادة الشهود، وفقاً للقواعد الإجرائية وقواعد الإثبات.

(84) انظر، على سبيل المثال، المفوضية السامية لحقوق الإنسان، *لجان التحقيق وبعثات تقصي الحقائق المعنية بالقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني: توجيهات وممارسات* ولا سيما الفصل الرابع-جيم بشأن جمع المعلومات وتقييمها.

(85) انظر Human Rights Center, University of California, Berkeley, School of Law, "Digital fingerprints: using electronic evidence to advance prosecutions at the International Criminal Court (Berkeley, 2014)". يمكن الاطلاع عليه في الرابط التالي: www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. والأدلة السماعية هي معلومات تقع خارج نطاق المعرفة المباشرة للشاهد الذي يدلي بشهادته. وفي بعض الولايات القضائية، تكون الأدلة السماعية غير مقبولة ما لم تلب استثناءً محدداً. وفي حالات أخرى، تكون هذه الأدلة مقبولة ولكن لا يقام لها وزن يذكر لأنه لا يمكن التحقق منها على النحو الواجب عند استجواب الشهود من قبل الادعاء أو الدفاع. ووفقاً لمنظمة الأمن والتعاون في أوروبا، "ومع أنَّ الأدلة السماعية تعد غير مقبولة بوجه عام في ولايات القانون العام القضائية إلا في حالة وجود ظروف خاصة، فإنَّ ولايات القانون المدني القضائية أو المحاكم الدولية لا تحظر هذه الأدلة". انظر Organization for Security and Cooperation in Europe, Mission to Bosnia and Herzegovina, *Investigation Manual for War Crimes, Crimes Against Humanity and Genocide in Bosnia and Herzegovina* (Sarajevo, 2013), p. 26. يمكن الاطلاع عليه في الرابط التالي: www.osce.org/bih/281491?download=true. وعلى الرغم من انعدام حواجز من هذا القبيل في ولايات القانون المدني القضائية وفي المحاكم الدولية، فإنَّ الأدلة السماعية يُنظر إليها، كقاعدة عامة، على أنها فئة غير موثوق بها بشكل خاص من الأدلة غير المباشرة، وغالباً ما يقيم القضاة لها وزناً ضئيلاً نسبياً.

بوضوح ودقة موقع ذلك المستند من القضية وكيف يمكن أن يتناسب معها[86].

60- وفي الحالات التي تعزى فيها المسؤولية عن الجرائم والانتهاكات إلى من هم في مستوى عالٍ من تسلسل القيادة، يمكن استخدام المعلومات التي تُجمع ليس فقط لتحديد "قاعدة الجريمة" (انظر أدناه) بل قد تكون مفيدة أيضاً في إثبات شكل مسؤولية[87] الجاني (الجناة) المدعى ارتكابه (ارتكابهم) الجريمة[88]. ويمكن اعتبار الأفراد مسؤولين عندما يُثبت كل عنصر من عناصر الجريمة أو الانتهاك، بما في ذلك الأفعال المادية (الأفعال الجرمية) والحالة العقلية للمتهم (القصد الجنائي) وفقاً لمعيار الإثبات المنطبق عليه. ولتحديد ذلك، يقوم متقصي الحقائق بفحص المعلومات المقدمة بشأن كل عنصر من عناصر الانتهاك أو الجريمة. وينبغي أن يكون المحققون على دراية بالجرائم أو الانتهاكات التي يمكن الادعاء بارتكابها وعناصر كل منها والمتهمين بارتكابها وبموجب أي نظرية للمسؤولية. وفي قضايا القانون الجنائي الدولي، غالباً ما يفصل الممارسون "الأدلة القائمة على الجريمة" عن "أدلة الربط". ويرد شرح لهذين المفهومين على النحو التالي:

(أ) الأدلة القائمة على الجريمة هي أدلة على الجرائم التي تستند إليها التهم، بما في ذلك معلومات عن: من وماذا وأين ومتى[89]. فعلى سبيل المثال، إن وُجِّهت إلى الجاني تهمة القتل بصفتها جريمة ضد الإنسانية، تُعد أي معلومة تثبت وقوع القتل دليلاً قائماً على الجريمة؛

(ب) أمَّا أدلة الربط فهي دليل على مسؤولية الجاني المزعوم عن الجرائم المرتكبة، وهو أمر يكتسي أهمية خاصة إن لم يرتكب الجاني الجريمة بشكل مباشر[90]. وبعبارة أخرى، هو الدليل الذي يربط الطرف المسؤول بالجريمة. فعلى سبيل المثال، في الحالات التي يكون فيها الادعاء بأنَّ أحد الرؤساء عجز عن منع الانتهاكات المزعومة التي كان على علم بها، أو عن المعاقبة عليها، تتمثل أدلة الربط في الأدلة التي تثبت هذا العلم، أو تثبت حقيقة أنَّ الرئيس كانت له "سيطرة فعلية" على الجاني المباشر.

(86) انظر، على سبيل المثال، المحكمة الدولية ليوغوسلافيا السابقة، *المدعي العام ضد بافل ستروغار*، القضية رقم IT-01-42-T، قرار بشأن مقبولية وثائق معينة، 26 أيار/مايو 2004، الدائرة الابتدائية الثانية، *والمدعي العام ضد ميلان ميلوتينوفيتش وآخرين*، القضية رقم IT-05-87-T، قرار بشأن التماس الادعاء قبول الأدلة المستندية، 10 تشرين الأول/أكتوبر 2006، الدائرة الابتدائية؛ المحكمة الجنائية الدولية لرواندا، *المدعي العام ضد إدوارد كاريميرا وآخرين*، القضية رقم ICTR-98-44-T، قرار بشأن طلب جوزيف نزيرويرا قبول وثائق من طاولة المحامين: بيانات ومحاضر علنية، 14 نيسان/أبريل 2009، الدائرة الابتدائية الثالثة؛ المحكمة الجنائية الدولية، *المدعي العام ضد توماس لوبانغا ديلو*، القضية رقم ICC-01/04/-01/06، قرار بشأن قبول مواد من "منصة المحامين"، 24 حزيران/يونيه 2009؛ المحكمة الدولية ليوغوسلافيا السابقة، *المدعي العام ضد رادوفان كارادزيتش*، القضية رقم IT-95-5/18-PT، أمر بشأن طلب الادعاء توضيحاً واقتراحاً بشأن المبادئ التوجيهية لإجراء المحاكمة، 20 تشرين الأول/أكتوبر 2009، الدائرة الابتدائية، *والمدعي العام ضد رادوفان كارادزيتش*، القضية رقم IT-95-5/18-T، قرار بشأن الالتماس الأول المقدم من الادعاء، 13 نيسان/أبريل 2010، الدائرة الابتدائية؛ المحكمة الجنائية الدولية، *المدعي العام ضد جيرمين كاتانغا وماثيو نغودجولو تشوي*، القضية رقم ICC-01/04-01/07، قرار بشأن التماسات منصة المحامين المقدمة من المدعي العام، 17 كانون الأول/ديسمبر 2010، الدائرة الابتدائية الثانية.

(87) Cryer, Robinson and Vasiliev, An Introduction to International Criminal Law and Procedure, chap. 15.

(88) انظر: *من المسؤول؟ إسناد المسؤولية الفردية عن انتهاكات القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني في لجان التحقيق، وبعثات تقصي الحقائق وغيرها من التحقيقات التابعة للأمم المتحدة* (نيويورك وجنيف، 2021). يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/sites/default/files/2023-01/AttributingIndividualResponsibility_AR.pdf.

(89) Kelly Matheson, Video as Evidence Field Guide (WITNESS, 2016), p. 42. يمكن الاطلاع عليه في الرابط التالي: https://vae.witness.org/video-as-evidence-field-guide.

(90) المرجع نفسه.

هاء- الحق في الخصوصية وحماية البيانات

61- الحق في الخصوصية حق أساسي من حقوق الإنسان[91]. ومن بين العناصر الهامة للحق في الخصوصية، الحق في حماية البيانات الشخصية الذي تكرسه مختلف قوانين حماية البيانات[92]. وعلى وجه الخصوص، تزداد أهمية قوانين حماية البيانات والخصوصية في التحقيقات التي تستخدم تكنولوجيا المعلومات والاتصالات الرقمية. وترد في ما يلي لمحة عامة وجيزة عن مفاهيم الحق الإنساني الدولي بشأن الخصوصية والإطار العالمي لحماية البيانات وأمنها وتبادل البيانات التي ينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على علم بها. وفي البيئة الرقمية، تكتسي الخصوصية المعلوماتية التي تشمل المعلومات الموجودة أو التي يمكن استخلاصها عن شخص ما، أهمية خاصة[93].

62- ويجب على المحققين المتخصصين في المصادر المفتوحة احترام حقوق الإنسان وأن يراعوا بشكل خاص الحق في الخصوصية الذي يرد ذكره كثيراً في سياق المعلومات الرقمية؛ فعلى سبيل المثال، يُعد انتهاك الحق في الخصوصية أحد الأسباب القليلة التي قد يستند إليها القضاة في استبعاد الأدلة في المحكمة الجنائية الدولية[94]. وتعزز الخصوصية الكرامة الإنسانية وغيرها من القيم الرئيسية، مثل حرية تكوين الجمعيات وحرية التعبير، وتحميها. وتقدم المحكمة الأوروبية لحقوق الإنسان بعضاً من أقوى التفسيرات لقوانين الخصوصية، مشفوعة بمجموعة تزداد بسرعة من الاجتهادات التي تعالج قضايا الحقوق الرقمية. وتؤدي انتهاكات هذه الحقوق الأساسية حتماً إلى أن يطعن الدفاع في الإجراءات الجنائية، بل وقد تشكل أسباباً مدنية لإقامة دعوى على أطراف التحقيق. وبالإضافة إلى قوانين الخصوصية، يساعد العديد من قوانين ولوائح حماية البيانات في تحقيق أمن البيانات الشخصية. وينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على دراية بوجه خاص باللائحة 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 نيسان/أبريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، وإلغاء التوجيه 95/46/EC (اللائحة العامة لحماية البيانات)، ونهجها في حماية البيانات الفردية، لأن هذا القانون وضع معياراً عالياً، وتنظر دول أخرى في اعتماد تشريعات مماثلة[95]. ومع ذلك، تختلف لوائح حماية البيانات من بلد إلى آخر، وتوجد اختلافات كبيرة وحتى قواعد متضاربة بشكل مباشر في بعض الأحيان. وينبغي للمحققين المتخصصين في المصادر المفتوحة استشارة خبير قانوني ليكونوا على وعي بقوانين ولوائح حماية البيانات المعمول بها ذات الصلة بالولايات القضائية التي يعملون فيها.

63- وفي الختام، ينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على دراية بالحظر العام المفروض على النفاذ غير المأذون به إلى البيانات والشبكات. فعلى سبيل المثال، يشمل ذلك استخدام كلمة مرور مسربة وجدت في مجموعة من البيانات المخترقة للحصول على مواد مقيدة،

(91) الحق في الخصوصية مدرج في العديد من صكوك حقوق الإنسان وفي القوانين الدستورية لأكثر من 130 بلداً. انظر، على سبيل المثال، الإعلان الأمريكي لحقوق الإنسان وواجباته، المادة الخامسة؛ الاتفاقية الأوروبية لحقوق الإنسان، المادة 8؛ الاتفاقية الأمريكية لحقوق الإنسان، المادة 11؛ اتفاقية حقوق الطفل، المادة 16؛ الاتفاقية الدولية لحماية حقوق جميع العمال المهاجرين وأفراد أسرهم، المادة 14؛ الميثاق الأفريقي لحقوق الطفل ورفاهيته، المادة 10؛ الميثاق العربي لحقوق الإنسان، المادتان 16 و21؛ إعلان رابطة أمم جنوب شرق آسيا بشأن حقوق الإنسان، المادة 21. انظر أيضاً Privacy International, "What is privacy?", 23 October 2017. يمكن الاطلاع عليه في الرابط التالي: https://privacyinternational.org/explainer/56/what-privacy.

(92) توجد قوانين لحماية البيانات في أكثر من 100 دولة وفي العديد من الصكوك الدولية والإقليمية. انظر، على سبيل المثال، Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data; Charter of Fundamental Rights of the European Union; Asia-Pacific Economic Cooperation Privacy Framework; Supplementary Act on Personal Data Protection within the Economic Community of West African States.

(93) انظر، عموماً، A/HRC/39/29، الفقرة 5.

(94) انظر نظام روما الأساسي، المادة 69(7).

(95) تنص اللائحة على أنَّ الأشخاص الطبيعيين يتمتعون بحقوق مرتبطة بحماية البيانات الشخصية وحماية معالجة البيانات الشخصية وحركة البيانات الشخصية غير المقيدة داخل الاتحاد الأوروبي. كما تنص اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية على حقوق مماثلة، ولا سيما بروتوكول عام 2018 الملحق بها. ولا تلزم الاتفاقية الدول الأعضاء في مجلس أوروبا فحسب، بل وعدداً من الدول الأخرى.

فضلاً عن النفاذ غير المأذون به إلى معلومات مقيدة بالخداع وغيره من أشكال الهندسة الاجتماعية[96].

واو- الاعتبارات القانونية الأخرى ذات الصلة

64- قد تنطبق قوانين أخرى في سياق التحقيقات المفتوحة المصدر. وترد أدناه قائمة غير حصرية ببعض الاعتبارات القانونية التي ينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على دراية بها.

1- انتهاك شروط الخدمة

65- تتضمن بعض تقنيات التحقيق الشائعة المفتوحة المصدر انتهاكات لشروط خدمة موقع شبكي أو منصة. فعلى سبيل المثال، ينتهك استخراج البيانات أو استخدام هوية افتراضية (لا هوية الشخص الحقيقية) شروط خدمة المنصات، وعلى وجه الخصوص، منصات التواصل الاجتماعي[97]. ويُعد انتهاك شروط الخدمة انتهاكاً لشروط العقد. وينبغي للمحققين أن يتأكدوا إن كان ذلك يشكل أيضاً عملاً غير قانوني في الولايات القضائية التي يعملون فيها. ويجب الموازنة بين الحاجة إلى الاستمساك بالمبادئ الأمنية التي قد يتيحها استخدام هويات افتراضية والضرر المحتمل الذي قد يؤدي إلى الإخلال بالعقد. وفي مثل هذه الظروف، يتمثل الرد الأكثر شيوعاً في تعطيل نفاذ المستخدم إلى المنصة. ولئن كانت الهويات الافتراضية ضرورية عند استخدامها حصراً للبحث في المصادر المفتوحة ورصدها على النحو المذكور أعلاه، فإنها ينبغي ألا تُستخدم لمحاولة النفاذ إلى محتوى مشترك على وسائل التواصل الاجتماعي الذي يخضع لضوابط نفاذ تقييدية؛ أو كذريعة للحصول على معلومات مباشرة من شخص باستخدام هوية مزيفة. ومن شأن سلوك من هذا القبيل أن يُخرج المحققين من نطاق التحقيق المفتوح المصدر وأن ينتهك المبادئ الأخلاقية[98] وقد ينتهك القانون[99].

2- قوانين الملكية الفكرية

66- ينبغي أن يكون المحققون على دراية بأي أذونات تتعلق بالملكية الفكرية قد يلزمهم الحصول عليها لنشر المعلومات التي جمعوها أثناء التحقيق و/أو توزيعها و/أو استخدامها بشكل قانوني. وتختلف القوانين ذات الصلة من ولاية قضائية إلى أخرى، وإن كانت معظم الولايات القضائية تتيح (كحد أدنى) لمنشئ المحتوى شكلاً من أشكال حماية حقوق الطبع والنشر، مثل مقطع فيديو أو صورة فوتوغرافية أو جزء من نص تتم مشاركته عبر الإنترنت. وعادة ما يتم تعريف "المنشئ" بأنَّه الشخص الذي أنشأ المادة فعلاً – على سبيل المثال، بالتقاط الصورة أو تسجيل الفيديو أو كتابة النص الأصلي – وليس الشخص الذي يقوم بالتحميل، على الرغم من أنهما قد يكونان شخصاً واحداً. وقد يلزم المستخدم النهائي الحصول على موافقة منشئ المحتوى على الاستخدام المقترح لتجنب انتهاك حقوق الطبع والنشر (على سبيل المثال، إن كان المحتوى سيُستخدم في تقرير عام أو رواية صحفية) – وعادة لا يكون الحصول على موافقة القائم بالتحميل، إن لم يكن هذا الشخص هو منشئ المحتوى أيضاً، كافياً لتجنب انتهاك القانون. وفي ذلك سبب آخر للحرص على تحديد المصدر الأصلي لكل جزء من المحتوى قد يحصل عليه المحققون. وتتيح بعض الولايات القضائية (وليس كلها) استثناءات لضرورة الحصول على الموافقة – وغالباً ما يسمى ذلك "الاستخدام العادل" أو استثناءات "التعامل العادل" – عندما تُستخدم مقاطع الفيديو والصور الفوتوغرافية والنصوص وغيرها من المعلومات لأغراض معينة مفيدة اجتماعياً، مثل التعليم، أو إنفاذ القانون، أو الصحافة. غير أنَّ هذه الاستثناءات، عند انطباقها، كثيراً ما تكون محدودة النطاق جداً، ومن ثم ينبغي ألا يُفترض قط أنَّ استخداماً بعينه يندرج في إطار هذا الاستثناء دون إجراء استعراض دقيق. وتشمل الآليات التي يمكن أن تساعد، في

(96) وفقاً لمعهد الولايات المتحدة الوطني المعني بالمعايير والتكنولوجيا، تمثل الهندسة الاجتماعية "فعل خداع شخص ليكشف عن معلومات حساسة من خلال التواصل معه لكسب الثقة والاطمئنان" (Paul A. Grassi, Michael E. Garcia and James L. Fenton, *Digital Identity Guidelines*, (Gaithersburg, Maryland, National Institute of Standards and Technology, 2017), 54). انظر أيضاً Michael Workman, "Gaining access with social engineering: an empirical study of the threat", *Information Systems Security*, vol. 16, No. 6(2007). For further discussion of unauthorized and deceptive access, see para. 65 below.

(97) على سبيل المثال، تتطلب شروط خدمة فيسبوك من المستخدمين "استخدام الاسم نفسه الذي يستخدمه الشخص في الحياة اليومية"، و"تقديم معلومات دقيقة عن نفسك" و"إنشاء حساب واحد فقط (حسابك الخاص) واستخدام الوقت المتاح لك لأغراض شخصية". انظر www.facebook.com/terms.php. وينتهك انتحال الشخصية قوانين تويتر وسياساته. انظر "Impersonation policy" على الرابط التالي: https://help.twitter.com/Ar/rules-and-policies/twitter-impersonation-policy.

(98) للاطلاع على مناقشة بشأن تزييف البيانات، انظر الفصل الثاني–جيم أعلاه بشأن المبادئ الأخلاقية.

(99) انظر الفصل الثالث–هاء أعلاه بشأن الحق في الخصوصية وحماية البيانات.

بعض الأحيان، في تقليل احتمال و/أو نطاق الانتهاك تضمين رابط يحيل إلى المحتوى الأصلي في تقرير رقمي دون إزالته من مصدره الأصلي وإسناد المحتوى إلى منشئه واستخدام جزء صغير فقط من المحتوى الأصلي – ومع ذلك، ينبغي التذكير مرة أخرى بأنَّ ذلك يعتمد على السياق والولاية القضائية.

وقد يكون للمعلومات الخاضعة لتراخيص المشاع الإبداعي، أو غيرها من التراخيص الحرة، مجموعة واسعة من الاستخدامات المسموح بها دون أي تكلفة. ومع ذلك، من المهم، إن كانت هذه التراخيص المجانية منطبقة، الامتثال لشروط الترخيص وعدم التعامل مع المحتوى بحسبانه لا يتطلب إذناً.

رابعاً

الأمن

موجز الفصل

- تقع مسؤولية أمن التحقيق والمتضررين منه على عاتق الجميع ولا تنحصر في المهنيين في مجال تكنولوجيا المعلومات فحسب.
- ينبغي أن تكون الاعتبارات الأمنية ذات شقين هما: (أ) شق يتعلق بالبنية الأساسية، بما في ذلك المعدات والبرمجيات والشبكات؛ (ب) شق يتصل بالسلوك ويشمل ذلك سلوك المحققين وجميع من يتواصلون معهم.
- ينبغي أن تُجرى التقييمات الأمنية على ثلاثة مستويات، هي مستوى المنظمة، والتحقيق المعيَّن/القضية المعيَّنة، والأنشطة/المهام المعيَّنة.
- ينبغي وضع تدابير حماية لتقليل الأخطار والتهديدات، على النحو المحدد في تقييم أخطار التحقيق.
- ينبغي أن تأخذ التقييمات الأمنية في الحسبان جميع أنواع الأضرار، بما في ذلك الضرر الرقمي والمالي والقانوني والبدني والنفسي الاجتماعي والضرر المتعلق بالسمعة.
- ترتبط بعض أكبر مواطن الضعف في التحقيقات المفتوحة المصدر باتصالات الإنترنت/عناوين بروتوكول الإنترنت، والأجهزة وميزاتها، وسلوك المستخدم.
- ينبغي للمحققين ومنظمات التحقيق أن تشارك في التدريب الأمني المستمر وفي نشر تدابير الحماية التي تتطور مع الطبيعة المتغيرة لأي تهديدات أو مواطن ضعف.

67- يتضمن هذا الفصل نظرة عامة عن اعتبارات الأمن عبر الإنترنت وخارجها ذات الصلة بالتحقيقات المفتوحة المصدر. وبفضل الإعداد المناسب والاستثمار والتركيز على تقييم التهديدات والتخفيف من حدة الأخطار، يُتوقع أن يكون المحققون المتخصصون في المصادر المفتوحة قادرين على تقليل أخطار إلحاق الضرر بالأشخاص والبيانات والأصول الأخرى إلى أدنى حد. وينبغي، قدر المستطاع، وضع الهياكل الأساسية الأمنية، ومن بينها الأجهزة والبرمجيات وبروتوكولات سلوك المستعملين، موضع التنفيذ قبل بدء التحقيق وتقييمها بانتظام واستكمالها، حسب الاقتضاء. وقد يكون لحجم المنظمة ومواردها تأثير في جدوى بعض تدابير الحماية. لذلك، يتضمن هذا الفصل معايير مرنة ينبغي تكييفها وفقاً لاحتياجات المنظمة والتحقيق المحددة. وينبغي للمنظمات التي تُجري تحقيقات شديدة الخطورة – مثل التحقيقات التي تشمل ضحايا ضعفاء بشكل خاص، أو في الحالات التي يكون فيها الجناة المدعى عليهم جهات فاعلة تابعة للدولة و/أو يتم تحديدهم بشكل فردي، أن تستعين بخدمات المهنيين ذوي الخبرة في مجال الأمن السيبراني. وبالإضافة إلى ذلك، ينبغي أن يتضمن الإطار الأمني المتين ضرباً من آليات المراجعة المستقلة والتدريب المستمر حتى يتمكن المستخدمون من مواكبة التطورات التكنولوجية الجديدة وأفضل الممارسات.

ألف- المعايير الدنيا

68- لأنَّ البنية التحتية الأمنية وأفضل الممارسات بشأن سلوك المستخدم لا تنفك تتغير، يقدم البروتوكول مبادئ شاملة يُبتغى منها أن يسترشد بها المحققون المتخصصون في المصادر المفتوحة في التفكير في مجال الأمن برمته. ويجب أن يتولى المحققون المسؤولية عن أمنهم، فيقيِّمون مستوى الأخطار التي يثيرها سلوكهم ويضعون تدابير كافية لتخفيف حدة الأخطار وللحماية منها. وعلى الرغم من الحاجة إلى اتباع نهج مخصص وفردي حيال الأمن، فثمة معايير دنيا يجب على المحققين المتخصصين في المصادر المفتوحة تطبيقها دائماً على عملهم، للامتثال لمبادئ الأمن وهي:

(أ) ينبغي للمحققين المتخصصين في المصادر المفتوحة تجنب الكشف عن عناصر محددة عن أنفسهم ومنظماتهم وأي شركاء أو مصادر لأطراف ثالثة ما لم يكن ذلك هدفاً أو التزاماً يقتضيه التحقيق. ولذلك، ينبغي للمحققين أن يحرصوا على عدم الكشف عن هويتهم على الإنترنت ويتأكدوا من عدم إسناد أنشطتهم على الإنترنت إلى أقصى حد ممكن؛

(ب) حري بالمحققين المتخصصين في المصادر المفتوحة أن يتوقعوا، عند إجراء أنشطة عبر الإنترنت، أن ترصد أطراف ثالثة هذه الأنشطة وتحللها. ولذلك، ينبغي لهم أن يضطلعوا بالأنشطة على الإنترنت بطريقة تتسق مع هوياتهم الافتراضية ولا تكشف عن هوياتهم أو أهدافهم التحقيقية، أو تعرض مصادرهم البشرية، أو أطراف ثالثة أخرى، لأخطار؛

(ج) يجب أن يدرك المحققون المتخصصون في المصادر المفتوحة أنَّ الإفراط في استغلال مصدر معلومات واحد عبر الإنترنت، مثل موقع معين، يزيد احتمال المراقبة والتحليل من طرف ثالث. ولذلك، حري بهم أن يتبعوا ممارسات تقلل إلى أدنى حد من هذا الاحتمال، مثل تنويع المصادر الرقمية؛

(د) يجب على المحققين المتخصصين في المصادر المفتوحة تجنب أنماط السلوك التي يمكن تحديدها أو التنبؤ بها، مثل أنماط البحث المتكررة على أجهزة يمكن التعرف عليها على نحو يساعد طرفاً ثالثاً على تحديد أهداف التحقيق ويجعل المحققين أهدافاً أسهل لهجمات استراق الهوية الرقمية وغيرها من أشكال الهندسة الاجتماعية[100]؛

(هـ) ينبغي للمحققين المتخصصين في المصادر المفتوحة إبقاء عملهم المهني منفصلاً عن الأنشطة الشخصية عبر الإنترنت. وينبغي تجنب استخدام الحسابات الشخصية لغايات التحقيق المهني عبر الإنترنت، وقدر المستطاع، الأجهزة الشخصية. وينبغي ألا تُستخدم معدات التحقيقات المهنية أبداً للأنشطة الشخصية عبر الإنترنت[101]؛

(و) ينبغي ألا يخلط المحققون المتخصصون في المصادر المفتوحة الذين يجرون تحقيقات متعددة بين تحقيقاتهم. ولذلك، ينبغي عليهم أن يخصصوا أوقات بداية ونهاية مختلفة لكل نشاط من أنشطة التحقيق وأن يحفظوا بيانات كل تحقيق ووثائقه في مواقع منفصلة ويستخدموا هويات افتراضية مختلفة، حسب الاقتضاء[102]؛

(ز) يجدر بالمحققين المتخصصين في المصادر المفتوحة استخدام أنظمة أو بيئات تقنية مصممة بحيث تتأثر إلى أدنى حد باحتمال إدخال برمجيات معادية أو ضارة أو غيرها من التأثيرات التخريبية التي قد تواجههم أثناء الأنشطة.

(100) انظر أدناه شرح هجمات استراق الهوية الرقمية والهندسة الاجتماعية.

(101) إن كان استخدام المعدات الشخصية أمراً لا مفر منه، فينبغي أن يُجري المستخدمون تحقيقات مهنية وأنشطة شخصية في بيئات منفصلة على الإنترنت، على سبيل المثال باستخدام جهاز افتراضي لتحقيقاتهم.

(102) بالإضافة إلى تقليل احتمال إرباك التحقيقات إلى أدنى حد، ستساعد هذه الممارسات بفعالية في الحفاظ على سلسلة المسؤولية.

باء- التقييمات الأمنية

69- لإعداد إطار أمني مناسب وفعال، يجب على المحققين المتخصصين في المصادر المفتوحة فهم مفاهيم الأمن السيبراني وإدارة الأخطار الرئيسية. ويلزم أيضاً أن يكونوا قادرين على تحديد الأصول التي تحتاج إلى حماية والأضرار المحتملة وتقييم التهديدات والأخطار ومواطن الضعف المحتملة.

70- وتتمثل الأخطار في احتمال فقدان أحد الأصول، أو اتلافه، أو تدميره نتيجة لتهديد يستغل ثغرة أمنية. ويرد أدناه تعريف لكل هذه المصطلحات. وبما أنَّ التحقيقات المفتوحة المصدر التي تجُرى على شبكة الإنترنت تتبع أساليب مختلفة لجمع المعلومات مقارنة بالتحقيقات التقليدية، فهي تثير أنواعاً مختلفة من الأخطار. ويشكِّل تحديد هذه الأخطار وتقييمها جزءاً أساسياً من التخطيط للتحقيق وإعداده. وتتضمن بعض الأمثلة على الأخطار الشائعة في التحقيقات المفتوحة المصدر ما يلي: القدرات التكنولوجية وإدراك الغاية من التحقيق، أو الكيانات التي تدعم تلك الغاية، والجهة التي يمكن أن تتهرب من التحقيق أو تضلله، ومشاكل الترتيب التقني لبيئة الإنترنت المستخدمة للتحقيق التي قد تؤدي إلى الكشف عن معلومات تمس بالتحقيق والبرمجيات أو الشفرات البرمجية الضارة التي قد تعرض أنظمة المحقق الحاسوبية، أو أنشطته، أو هويته، أو البيانات المجمعة لأخطار، أو الميزات التقنية، مثل أجهزة التتبع وملفات تعريف الارتباط والإشارات والتحليلات التي قد تُعرِّض أنشطة التحقيق لأخطار.

71- ويتضمن الفرع التالي تفسيرات للمصطلحات الرئيسية ولتطبيقها على التحقيقات المفتوحة المصدر، مما يتيح خريطة طريق لتقييم التهديدات والأخطار.

1- الأصول

72- الأصل هو أي شيء يحتاج إلى الحماية ويشمل ذلك الأشخاص[103] والممتلكات والمعلومات. وفي سياق التحقيقات المفتوحة المصدر، يجوز أن يشمل ذلك الأشخاص الذين يحتاجون إلى الحماية والمحققين أو أفرقة التحقيق، بما في ذلك أي شخص يعمل معه المحققون أو أفرقة التحقيق (أي الزملاء الداخليون والشركاء الخارجيون، المحليون منهم والعاملون في الميدان على حد سواء) والمؤلفون أو مصادر المعلومات والشهود والضحايا والجناة المزعومون وغير المشاركين في التحقيق. وتتألف الممتلكات من عناصر ملموسة وغير ملموسة يمكن إعطاء قيمة لها[104]. وتشمل الأصول الملموسة المباني والمعدات والمستندات. أما الأصول غير الملموسة فتتكون من السمعة ومعلومات الملكية، مثل البيانات الرقمية والبيانات الوصفية وقواعد البيانات وشفرة البرمجيات والسجلات.

2- الضرر

73- يتألف الضرر من ضرر بدني، أو عقلي، أو إضرار بالأصول، أو تدميرها. وهو قد يتخذ شكل ضرر رقمي، أو مالي، أو قانوني، أو مادي، أو نفسي اجتماعي، أو إضرار بالسمعة.

(أ) الضرر الرقمي

74- يشير الضرر الرقمي إلى الضرر الذي يلحق بأي معلومات، أو بنية تحتية رقمية. ويشمل الضرر الرقمي المحتمل تدمير البيانات، أو المساس بها، أو فقدانها، أو تعطيل الخدمات من أنظمة الحاسوب ومنصاته.

(ب) الضرر المالي

75- يمكن أن ينشأ الضرر المالي من مصادر عديدة من بينها الضرر القانوني والمساس بالسمعة المرتبط بالتحقيق. وقد يتعرض المحققون والأهداف ومن لا يشاركون في التحقيق جميعاً لمثل هذا الضرر. وبالإضافة إلى ذلك، قد يقع ضرر مالي عندما يعجز المحققون عن تقدير تكاليف التحقيق الطويلة الأجل بشكل كاف.

(ج) الضرر القانوني

76- قد يتحمل المحققون المتخصصون في المصادر المفتوحة مسؤولية قانونية، إما عن أسلوب عملهم، أو عن حصيلته. وحري بالمحققين أن يكونوا على دراية بالقيود القانونية المفروضة على ما يسمح لهم به من أفعال وبالتداعيات القانونية لأفعالهم، نشدانا لتقليل أخطار المسؤولية القانونية لأنفسهم و/أو أطراف ثالثة. ويمكن أن تعرِّض التحقيقات أيضاً من يخضعون لها، بل وغير المشاركين في التحقيق الذين ربما

(103) لا يُشار إلى الأشخاص بصفتهم أصولا إلّا في سياق إجراء تقييمات أمنية.

(104) انظر Threat Analysis Group, "Threat, vulnerability, risk - commonly mixed up terms" يمكن الاطلاع عليه في الرابط التالي: www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

وقعوا في أخطاء قانونية لم يُكشف عنها أثناء التحقيق، لضرر قانوني[105].

(د) الضرر المادي

77- يشمل الضرر المادي الضرر الذي يلحق بالأفراد، أو يصيب الممتلكات. وبما أنَّ المحققين المتخصصين في المصادر المفتوحة عادة ما يزاولون عملهم من مكتب أو منزل، بدلاً من الخروج إلى الميدان، فإنَّ الضرر المادي ينبغي أن يُقيَّم بحسبانه نتيجة يحتمل أن تسفر عنها الأنشطة المجراة عبر الإنترنت. ويمكن أن يكون للإجراءات المتخذة في الفضاء السيبراني عواقب في العالم الحقيقي يجدر بالمحققين أن يكونوا على دراية بها وأن يعدوا العدة لها. فعلى سبيل المثال، ينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على علم بالأفراد الموجودين في بيئات غير آمنة وقد يتعرضون لأذى مادي بسبب سلوك المحقق على الإنترنت، سواء أكان هؤلاء الأفراد زملاء للمحققين، أو مستخدمين للإنترنت في بلدان الحالة المعنية، أو غيرهم. ويقع على المحققين عبر الإنترنت واجب أخلاقي – وقانوني في بعض الحالات – هو واجب الرعاية[106] حيال الآخرين حتى لا يصبح المعرضون للضرر المادي أكثر عرضة له بسبب أنشطة المحققين. وينبغي أن تُعدَّ الأخطار المادية جزءاً من تقييم شامل للتهديدات يُجرى قبل بدء العمل ويعاد تقييمه طوال فترة التحقيق.

(هـ) الضرر النفسي الاجتماعي

78- يتراوح الضرر النفسي الاجتماعي بين الضائقة النفسية والصدمة النفسية. وهو قد يصيب أي عضو في فريق التحقيق و/أو الأشخاص المشاركين فيه أو المتأثرين به، بما في ذلك الخاضعون للتحقيق وغير المشاركين فيه. وفضلاً عمَّا لحماية الذات والآخرين من الضرر النفسي من أهمية أخلاقية ومعنوية، ثمة حالات يمثل فيها العنصر البشري أوهن الحلقات في أداء أي منظمة عملها بشكل فعال. فقد يكون الشخص المصاب بضرر نفسي ضعيفاً بوجه خاص، فيتيح فرصاً جديدة تستغلها الجهات الفاعلة المهدِّدة، أو يثير أخطار أخرى تهدد الأمن المادي والرقمي، لا سيما إن أحدثت التأثيرات النفسية السلبية ضعفاً في الأداء، مثل التراخي أكثر من المعتاد في الالتزام بالبروتوكولات الأمنية. ومعلوم أنَّ مشاهدة كميات كبيرة من مقاطع الفيديو العنيفة أو مقاطع الفيديو الصادمة عملية يصعب تحملها بشكل خاص وقد تتسبب في ضائقة نفسية أو صدمة نفسانية تستوجب دعماً مهنياً. ومن علامات الصدمة الثانوية التغيرات التي تحدث في السلوك وتقلب المزاج والتحولات في عادات الأكل أو الشرب وفقدان القدرة على النوم والرغبة في النوم أكثر من المعتاد أو الكوابيس[107]. ويرد بيان لاستراتيجيات تخفيف الضرر النفسي في الفرع الخاص بإعداد وإنشاء خطة للتحمل والرعاية الذاتية[108].

(و) الإضرار بالسمعة

79- يكون الإضـرار بالسمعة، في سياق التحقيقات المفتوحة المصدر، أشد وطأة على المحققين و/أو منظماتهم، على سبيل المثال، في الحالات التي ينشر فيها المحققون معلومات خاطئة، أو ينتهكون الأخلاقيات، أو ينتجون محتوى إشكالياً. وقد يلحق الإضرار بالسمعة أيضاً بمن يخضعون للتحقيقات الذين قد يواجهون وصمة عار بسبب سلوكهم المزعوم إثر الإعلان عن هذا السلوك. ويثير هذا الأمر القلق بوجه خاص حين تُوجَّه إلى أشخاص، أو منظمات، اتهامات يتبين فيما بعد أنها كاذبة.

3- تدابير الحماية

80- تدابير الحماية هي الجهود المبذولة لتفادي مواطن الضعف، أو تقليلها، وهي تشمل تدابير مادية وتكنولوجية وسياساتية.

(105) انظر أيضاً الفصل الرابع–هاء والرابع–واو أعلاه لمزيد من النقاش بشأن الاعتبارات القانونية ذات الصلة.

(106) نظام روما الأساسي، المادة 54(1)(ب).

(107) انظر Dart Center for Journalism and Trauma, "Working with traumatic imagery", 12 August 2014 (available at https://dartcenter.org/content/working-with-traumatic-imagery)؛ Sam Dubberley, Elizabeth Griffin and Haluk Mert Bal, *Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline* (Eyewitness Media Hub, 2015). يمكن الاطلاع عليه في الرابط التالي: http://eyewitnessmediahub.com/research/vicarious-trauma)؛ Sam Dubberley and Michele Grant, "Journalism and vicarious trauma: a guide for journalists, editors and news organisations" (First Draft News, 2017). (يمكن الاطلاع عليه في الرابط التالي: https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf)؛ Center for Human Rights and Global Justice, "Human rights resilience project launches new website", 21 May 2018. (يمكن الاطلاع عليه في الرابط التالي: https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website)؛ Keramet Reiter and Alexa Koenig, "Reiter and Koenig on challenges and strategies for researching trauma", Palgrave MacMillan (يمكن الاطلاع عليه في الرابط التالي: www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

(108) انظر الفصل الخامس–دال أدناه لمزيد من المعلومات عن الرعاية الذاتية.

وتشمل الحماية المادية وضع أقفال على المباني، أو الغرف، أو الخزانات التي تُخزَّن فيها مواد حساسة. وتتضمن التدابير التكنولوجية استخدام كلمات المرور والتشفير والمصادقة المتعددة العوامل على الأجهزة، أو ضوابط النفاذ إلى أنظمة البيانات. وتتألف تدابير السياسة العامة من القواعد الداخلية والخارجية والقوانين وآليات الإنفاذ، مثل قواعد منع إرسال منتج عمل داخلي من بريد إلكتروني خاص بالعمل إلى بريد إلكتروني شخصي، أو السياسات المتعلقة بمنع استخدام حسابات وسائل التواصل الاجتماعي الشخصية على حاسوب الشخص المخصص للعمل.

4- التهديدات

81- التهديدات هي كل شيء ينبغي حماية الأصول منه. ويتمثل التهديد في كل ما يمكن أن يستغل ثغرة أمنية، عمداً أو خطأً، ويحصل على أصل، أو يتلفه، أو يدمره. وقد تكون التهديدات التي تتعرض لها منظمة، أو تحقيق، داخلية أو خارجية يتولى تنفيذها أفراد، أو مجموعات، أو مؤسسات، أو شبكات. وينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على دراية، من بين أمور أخرى، بالتهديدات التالية.

(أ) هجمات الحرمان من الخدمة الموزعة

82- هجمات الحرمان من الخدمة الموزعة هي هجمات سيبرانية مصممة لشل قدرة الجهة المستهدفة على النفاذ إلى جهاز، أو شبكة. وينبغي وضع نظام لتخفيف حدة هذه الهجمات، حماية للأصول الموجهة للجمهور، مثل المواقع الشبكية وغيرها من بوابات النفاذ عن بعد. وبالإضافة إلى ذلك، ينبغي وضع نظام لتسجيل الحوادث واستخدامه عند وقوع هجوم لتسجيل جميع الأفعال والجهات الفاعلة لها.

(ب) هجمات استراق الهوية الرقمية

83- استراق الهوية الرقمية هو محاولة احتيالية للحصول على معلومات حساسة، مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان، من خلال التنكر في هيئة جديرة بالثقة في اتصال إلكتروني[109]. وتُستخدم عمليات استراق الهوية الرقمية، أو الاحتيال عبر الهاتف، للحصول على معلومات سرية، أو لمضايقة المحققين. وبوجه عام، تكون الحسابات الشخصية أكثر عرضة من الحسابات المهنية. لذا، فقد يُعرِّض استخدامها التحقيقات، أو مُنتَج العمل، لأخطار.

(ج) هجمات المتسلل

84- هجمات المتسلل هي نوع من الهجمات السيبرانية تتسلل فيها جهات فاعلة خبيثة إلى محادثات بين طرفين وتنتحل شخصية كليهما لتنفذ إلى المعلومات التي كان الطرفان يحاولان إرسالها إلى بعضهما إلى بعض[110]. ويتيح هجوم المتسلل للجهة الفاعلة الخبيثة اعتراض البيانات المخصصة لشخص آخر وإرسالها وتلقيها، أو البيانات التي لا يقصد إرسالها على الإطلاق، دون أن يعلم بذلك أي من الطرفين الخارجيين إلا بعد فوات الأوان[111].

(د) الهندسة الاجتماعية

85- الهندسة الاجتماعية هي التلاعب النفسي بالأشخاص لحملهم على القيام بعمل ينطوي على ضرر، مثل الكشف عن معلومات سرية. والأمثلة على الهندسة الاجتماعية كثيرة ومختلفة، من بينها استراق الهوية الرقمية الموجه[112]. وبما أنَّ أساليب الهندسة الاجتماعية لا تنفك تتطور، وجب على المحققين الحرص على التدريب المستمر على اكتشاف أساليب الهندسة الاجتماعية وسبل تفاديها.

(هـ) البرمجيات الخبيثة

86- تشير البرمجيات الخبيثة إلى برامج الحاسوب المصممة للتسلل إلى أجهزة الحاسوب وإتلافها دون موافقة المستخدم. وتوجد أنواع عديدة من البرمجيات الخبيثة، مثل برمجيات التجسس الحاسوبي وبرمجيات انتزاع الفدية.

5- الجهات الفاعلة المهدِّدة

87- الجهة الفاعلة المهدِّدة، أو الجهة الفاعلة المضرّة، هي شخص، أو كيان، مسؤول عن حدث، أو حادث، له تأثير في سلامة، أو أمن، كيان أو جهة فاعلة أخرى، أو لديه القدرة على التأثير فيه. وفي التحقيقات الجنائية الدولية وتحقيقات حقوق الإنسان، يُرجَّح أن تكون الجهات الفاعلة المهدِّدة هي الجناة

(109) انظر Phishing.org, "What is phishing?". يمكن الاطلاع عليه في الرابط التالي: www.phishing.org/what-is-phishing.

(110) انظر Veracode, "Man in the middle (MITM) attack". يمكن الاطلاع عليه في الرابط التالي: www.veracode.com/security/man-middle-attack.

(111) المرجع نفسه.

(112) استراق الهوية الرقمية الموجه هو ممارسة احتيالية تتمثل في إرسال رسائل بريد إلكتروني تكون في ظاهرها من مرسل معروف أو موثوق به لحث الأفراد المستهدفين على الكشف عن معلومات سرية.

المدعى عليهم، أو أهداف التحقيق، بما في ذلك الحكومات، أو مؤيدوها. ومن المهم أن يحدد المحققون المتخصصون في المصادر المفتوحة الجهات الفاعلة المهدِّدة المحتملة وأن يدركوا قدراتها واحتمال أن تقوم بشن هجمات.

6- قابلية التضرر

88- تشكِّل قابلية التضرر موطن ضعف، أو فجوة، في تدابير الحماية توجد في كلا المجالين الرقمي والمادي. وفي الأنشطة عبر الإنترنت، تشمل قابلية التضرر موطن ضعف في تدابير الحماية الأمنية يمكن استغلاله للنفاذ غير المأذون به إلى أحد الأصول والعيوب الأمنية التي تشوب البرمجيات والتصميم غير المأمون والمستخدمين المتمتعين بامتيازات مفرطة والشفرات البرمجية. وفي وضع عدم الاتصال، تشمل قابلية التضرر أيضاً نقاط ضعف لدى الأشخاص، كأن يكون أحد أعضاء الفريق قابلاً للابتزاز، أو الإكراه، أو قد يصاب بضعف نتيجة التعرض المفرط لمواد صادمة أو بسبب ظروف عمل شاقة أخرى[113]. ويمكن إحداث نقاط ضعف جديدة بالكشف للمستهدف عن مجرى تحقيق جار أو نطاقه. وفي الختام، قد تنشأ الثغرات الأمنية عن تهديدات خارجية، مثل البرمجيات الخبيثة والفيروسات الجديدة التي ينبغي على المحققين أن يكونوا على علم بها. وينبغي أن تؤخذ هذه الأنواع من مواطن الضعف في الحسبان عند حصر الأخطار وتقييمها.

89- وينبغي أن يكون المحققون المتخصصون في المصادر المفتوحة على دراية بمواطن الضعف التالية في الإنترنت.

(أ) ملفات تعريف الارتباط

90- ملف تعريف الارتباط هو ملف صغير غالباً يُرسل عبر موقع شبكي ويُخزن إما في ذاكرة حاسوب المستخدم، أو يُكتب على قرص الحاسوب ليستخدمه المتصفح. وغالباً ما تكون ملفات تعريف الارتباط ضرورية ليؤدي الموقع الشبكي عمله بشكل سليم – على سبيل المثال، بإتاحة القدرة على تخزين أفضليات الموقع الشبكي وتفاصيل هوية المستخدمين لتفادي الحاجة إلى إدخال البيانات بشكل متكرر أثناء الزيارات اللاحقة. وتُعد ملفات تعريف الارتباط بحيث تتمكن من جمع وتخزين بيانات مهمة – غالباً ما تكون حساسة – عن الزوار وزياراتهم. وتطور بعض هذه الملفات إلى أدوات مركزية يمكن استخدامها لجمع بيانات يستعان بها في رسم صورة عن اهتمامات المستخدم والعادات التي يتبعها في التصفح. ويظل ملف تعريف الارتباط موجوداً على جهاز الحاسوب حتى تنتهي صلاحيته أو يحذفه المستخدم.

(ب) المتتبِعات

91- المتتبِّع هو نوع من ملفات تعريف الارتباط يستغل قدرة المتصفح على الاحتفاظ بسجل لصفحات الموقع الشبكي التي تمت زيارتها وبمعايير البحث التي أُدخلت، وما إلى ذلك. والمتتبعات هي ملفات تعريف ارتباط دائمة تحتفظ بسجل تشغيلي لسلوك من يزور الموقع الشبكي. وتقوم المتتبعات في أبسط أشكالها بتعيين هوية فريدة لمتصفح المستخدم، ثم تربط هذه الهوية بجميع أنشطة التصفح والبحث اللاحقة (معايير البحث والصفحات التي تمت زيارتها وتسلسل الصفحات التي تمت زيارتها، ونحو ذلك)، فتتاح بذلك لمالك المتتبع القدرة على ربط الزيارات السابقة واللاحقة معاً بموقع شبكي (أو مجموعة من المواقع الشبكية التابعة) لتكوين صورة مفصلة عن المستخدمين وعادات التصفح الخاصة بهم. وغالباً ما تُضمَّن المتتبعات في الإعلانات التي تُوزَّع بعد ذلك عبر مواقع شبكية متعددة، فتتاح للمتتبع فرصة أكبر بكثير لمعرفة نشاط المستخدم وسلوكه. وحتى زيارة موقع شبكي "موثوق به" قد يؤدي إلى تثبيت متتبعات على حواسيب المستخدمين وتتبع أنشطتهم اللاحقة على الإنترنت.

(ج) المرشدات

92- المرشد هو آلية لتتبع نشاط المستخدم وسلوكه. ويتم إنشاء المرشدات من عنصر صغير لا يثير الإزعاج (غالباً ما يكون غير مرئي) في صفحة موقع شبكي (شيء صغير مثل بكسل شفاف واحد) يؤدي، عند تقديمه بواسطة متصفح، إلى إرسال تفاصيل عن هذا المتصفح وحاسوبه إلى طرف ثالث. ويمكن استخدام المرشدات جنباً إلى جنب مع ملفات تعريف الارتباط لتفعيل جمع البيانات ونقلها وتحديد المستخدمين بشكل فريد وتسجيل عاداتهم في التصفح. وترتبط المرشدات ارتباطاً وثيقاً بمواقع التواصل الاجتماعي حيث يشكّل تحديد العلاقات والشبكات اللبنات الأساسية للمواقع الشبكية. وختاماً، تُستخدم المرشدات داخل البريد الإلكتروني المستند إلى لغة الترميز المستخدمة في الوثائق لجمع هوية المستخدم والإبلاغ عنها والنفاذ إلى أي ملفات تعريف ارتباط خُزِّنت مسبقاً على ذلك الحاسوب.

(د) الشفرات البرمجية والبرامج النصية الأخرى

93- يستخدم عدد متزايد من المواقع الشبكية أجزاءً صغيرة من الشفرات البرمجية يقوم المتصفح الذي يستخدمه الزائر بتنزيلها وتكون قادرة على تخزين معلومات عن الزيارة. ويمكن أن تؤثر هذه الشفرات البرمجية في الشكل الذي يظهر به الموقع الشبكي وكيفية تفاعله مع المدخلات واستجابة المتصفح للموقع الشبكي. والشفرة البرمجية قادرة أيضاً على تخزين بيانات حساسة تتعلق ببيانات اعتماد الزوار وأنشطتهم، وما إلى

(113) انظر الفصل الخامس–دال أدناه للحصول على مزيد من المعلومات عن القدرة على التحمل والرعاية الذاتية.

ذلك. وقد يكون جمع البيانات مستمراً وتُرسل البيانات إلى طرف ثالث.

جيم- الاعتبارات المتصلة بالبنية التحتية

94- تشير البنية التحتية إلى الهياكل والمرافق والأنظمة اللازمة لإجراء تحقيقات مفتوحة المصدر، بما في ذلك البرمجيات والأجهزة على حد سواء. وينبغي أن تتيح البنية التحتية تدابير أمنية كافية لحماية أصول المنظمة وبياناتها وصونها (وأن تزود بهذه التدابير). وحتى تكون البنية التحتية قادرة على التحمل، ينبغي أن تُوضع تدابير تخفيف تضمن الاستمرارية، إن حدث أي مما يلي:

(أ) انقطاع الاتصال بالإنترنت، أو فقدانه؛

(ب) تعطيل النفاذ إلى البيانات المخزنة، أو فقدانه؛

(ج) فقدان البيانات، أو تلفها، أو تدميرها؛

(د) تعطل خدمات البرمجيات، أو فقدانها؛

(هـ) تلف الأجهزة، أو فقدانها؛

(و) النفاذ غير المأذون به إلى الأجهزة؛

(ز) النفاذ غير المأذون به إلى الشبكة؛

(ح) الحذف العرضي للبيانات، أو المساس بها؛

(ط) تدمير البيانات، أو المساس بها عمداً؛

(ي) تسرب البيانات، أو احتجاز البيانات "رهينة".

95- وتُحدد البنية اللازمة حسب حجم أنشطة التحقيق عبر الإنترنت التي يتعين القيام بها وطبيعة التحقيق وموضوع الاهتمام، فضلاً عن الموارد المالية المتاحة لإنشاء البنية التحتية واستدامتها وتعديلها حسب الحاجة.

1- البنية التحتية

96- تشمل البنية التحتية المستخدمة في التحقيقات المفتوحة المصدر المكونات التالية كحد أدنى، مع إضافة خصائص ذات صلة باستراتيجيات تحقيق محددة.

(أ) الأجهزة

97- يجب أن يكون لدى المحققين المتخصصين في المصادر المفتوحة معدات تتيح النفاذ إلى المحتوى المنشور على الإنترنت، سواء أكان حاسوباً مكتبياً، أو حاسوباً محمولاً، أو جهازاً لوحياً، أو هاتفاً ذكياً. وينبغي أن تكون الأجهزة والمعدات محمية بكلمة مرور ومزودة بتشفير كامل للقرص، وأن تستخدم، في الحالة المثلى، المصادقة المتعددة العوامل[114]. وينبغي نسخ جميع المعدات احتياطياً بانتظام. وعندما لا تكون الأجهزة قيد الاستخدام، يجب تخزينها بشكل آمن مع قصر النفاذ إليها على المستخدم والموظفين المعتمدين. وينبغي ألا تُستخدم المعدات الشخصية في أنشطة العمل. وبالمثل، ينبغي ألا تُستخدم معدات التحقيق في الأنشطة الشخصية لاحتمال ربط وسائل التواصل الاجتماعي الشخصية بالهويات الافتراضية المنشأة لغرض التحقيق[115].

(ب) الاتصال بالإنترنت

98- من الناحية المثالية، يكون لدى المحققين اتصال بالإنترنت قوي ومستقر وخاص. وينبغي عليهم تجنب استخدام تقنية الاتصال اللاسلكي العامة. ومع أنَّ تقنية الاتصال اللاسلكي المجانية والعامة، بما في ذلك الشبكات شبه الخاصة، مثل الشبكات التي تتيحها الفنادق، أو مقاهي الإنترنت، تتيح خياراً مناسباً، فإنَّها غير آمنة للغاية وعرضة لتهديدات عديدة أشدها وطأة قدرة قراصنة الحواسيب على وضع أنفسهم بين المستخدم ونقطة الاتصال. ويتطلب استخدام نقطة اتصال شخصية محمية بكلمة مرور استثماراً مالياً، ولكنه ضروري لإجراء أنشطة تحقيق آمنة عبر الإنترنت. وبالإضافة إلى ذلك، يُفضَّل، من منظور الوظائف والأمان معاً، وجود اتصال قوي ومستقر بالإنترنت. غير أنَّ ذلك لا يعتمد على إرادة المحقق على الدوام. وفي حالة استخدام شبكة افتراضية خاصة على رابط اتصال غير مستقر، يجدر بالمحققين وضع آلية آمنة تحمي من التعطل حتى لا يُكشف عن عنوان بروتوكول الإنترنت خاصتهم إن انقطع الاتصال.

(114) تمثل المصادقة المتعددة العوامل تعزيزاً أمنياً يتطلب من المستخدم تقديم نوعين من بيانات الاعتماد لتسجيل الدخول إلى حساب. على سبيل المثال تقديم كلمة المرور والقياسات الحيوية (بصمات الأصابع) أو بطاقة ذكية. انظر United States, National Institute of Standards and Technology, "Back to basics: multi-factor authentication (MFA)". يمكن الاطلاع عليه في الرابط التالي: www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

(115) قد يصعب الامتثال لهذه التوصية أثناء السفر، لأن العديد من المحققين سيحضرون معهم أجهزة عملهم ولكنهم يرغبون في القيام بأعمال شخصية خارج ساعات العمل، أو يحتاجون إلى ذلك. لذا، يجدر بالمنظمات التي تُجري تحقيقات مفتوحة المصدر أن تضع سياسات سفر معقولة.

(ج) متصفحات الشبكة

99- يندرج متصفح الشبكة المستخدم في استقصاء المواقع الشبكية على الإنترنت والبحث عنها والنفاذ إليها في عداد الأدوات الأساسية التي تستخدمها التحقيقات عبر الإنترنت. وتعمل المتصفحات كواجهة بينية أساسية بين المحققين والإنترنت، وهي غالباً ما لا تؤخذ في الحسبان بصفتها مصدراً للأخطار. وتُعدَّل المتصفحات الحديثة باستمرار وهي تتضمن مجموعة واسعة من الوظائف المدمجة لاستيعاب العديد من المتطلبات. وتعد المتصفحات أيضاً هدفاً رئيسياً لمن يرغبون في مراقبة خصم، أو في شن هجمات عليه، إذ يمكن إساءة استخدام الوظائف وإضافة وظائف إضافية بسهولة نسبية. ويقوم المتصفح بالنفاذ المتزامن إلى الإنترنت والحاسوب، ومن ثم يكون بمقدوره تحديد معلومات عن المستخدم. ومن شأن تسرب البيانات عبر المتصفح أن يكشف النقاب عن بيانات كافية لتنبيه من يخضع للتحقيق. وتحتوي المتصفحات الحديثة على ميزات عديدة مضمنة فيها قد تضاف إليها ميزات أخرى عديدة تُسمى وظائف المتصفح الإضافية من شأنها أن تسرب البيانات بشكل فردي، أو جماعي، يؤدي إلى تحديد هوية التحقيق، أو المحقق، أو مسار التحقيق، وأنشطة البحث المرتبطة به. والمتصفحات أيضاً قادرة، بطبيعتها، على تنزيل الشفرة الحاسوبية المستمدة من موقع شبكي وتطبيقها. وقد لا يكون وجود و/أو وظيفة الشفرة الحاسوبية مرئياً للمحققين. ومع ذلك تستطيع الشفرة الحاسوبية تغيير المحتوى الرقمي الذي يُرسل إلى المحققين والنفاذ إلى الوظائف والبيانات الموجودة على حواسيبهم، بل وجعل الحواسيب تتصرف بشكل يخالف الشكل المراد لها. وينبغي أن يسعى المحققون المتخصصون في المصادر المفتوحة إلى تقليل هذه الأخطار إلى أدنى حد باستخدام متصفحات آمنة ومحدثة تُفحص بانتظام والاستعانة بالبرمجيات والمكونات الإضافية المناسبة المركبة التي تخفف من حدة بعض الأخطار المبيَّنة أعلاه[116].

2- التدابير الأمنية

100- يمكن استخدام عناصر البنية التحتية الأساسية هذه لتحديد المستخدمين ومواقعهم. وحتى يمتثل المحققون لمبدأ عدم الكشف عن هويتهم وعدم الإسناد، ينبغي أن يستخدم المحققون الاستراتيجيات التالية لتمويه اتصالاتهم بالإنترنت. وتخفي هذه الاستراتيجيات الموقع وعنوان بروتوكول الإنترنت وتموه الجهاز وتخفي ميزاته التعريفية ونظام التشغيل والمتصفح.

(أ) تمويه الاتصال

101- يمكن لعنوان بروتوكول الإنترنت إفشاء معلومات قد تُستخدم لاستهداف بنية المؤسسة التحتية. وينبغي أن يسعى المحققون المتخصصون في المصادر المفتوحة إلى استخدام شبكات افتراضية خاصة، أو بيانات غير مباشرة، أو غيرها من البرمجيات، لإخفاء عناوين بروتوكول الإنترنت الخاصة بحواسيبهم. ويعني ذلك أنَّ عناوين بروتوكول الإنترنت التي تُكشف للإنترنت لا تكون مرتبطة بالمحققين، أو بمنظماتهم. وتنشئ الشبكات الافتراضية الخاصة أيضاً قناة مشفرة للاتصالات بين حاسوب المحقق وخادوم الشبكة الافتراضية الخاصة بحيث لا تُرى أي شبكات/عُقد يمر بها الاتصال سوى البيانات المشفرة، واضعة بذلك طبقة إضافية من الحماية. ومع ذلك، تحظر بعض البلدان والمواقع الشبكية استخدام بعض الشبكات الافتراضية الخاصة وقد تشير إلى أطراف ثالثة بأنَّ أنشطة التحقيق قد تكون أنشطة مشبوهة. وفي الوضع المثالي، يتوقع أن تتيح الشبكات الافتراضية الخاصة للمحققين استخدام عناوين عديدة لبروتوكول الإنترنت وتمكنهم من التبديل بينها بسرعة عند الضرورة. وينبغي ألا تعزى عناوين بروتوكول الإنترنت إلى بلد واحد، بل يجب توزيعها بحيث تعبر عن مواقع متعددة في مختلف أنحاء العالم.

(ب) تمويه الجهاز

102- لإخفاء بعض الميزات التي قد تُستخدم لتحديد هوية المستخدمين، يستطيع المحققون استخدام أجهزة افتراضية، أي برمجيات، أو أنظمة تشغيل، تُظهر سلوك أجهزة حاسوبية متميزة. وبشكل أساسي، سيؤدي استخدام جهاز افتراضي إلى إنشاء حاسوب جديد داخل الحاسوب – أي إنشاء بيئة منفصلة تماماً عن بقية الحاسوب. ويكون الجهاز الافتراضي قادراً أيضاً على أداء مهام من قبيل تشغيل التطبيقات والبرامج وكأنه حاسوب منفصل تماماً[117]، فيظهر المحقق الذي يستخدمه كشخص مختلف على الإنترنت. وعند استخدام جهاز افتراضي، يُتاح للمحققين نظام لتغيير المتصفح ووكيل المستخدم والبرمجيات والمنافذ المفتوحة ونظام التشغيل وغيرها من المعلومات عن الجهاز حتى يظهروا في شكل أشخاص مختلفين في كل مرة يستخدمون فيها الإنترنت. وفي أفضل الحالات، يُتوقع أن تتيح البنية التحتية للمحقق استخدام جهاز افتراضي يخفي الجهاز الفعلي الذي يستخدمه. ويمكن تدمير الأجهزة الافتراضية وإعادة إنشائها، أو إعادتها إلى نقطة سابقة، أو تكوينها بطرق مختلفة، أو تكرارها لحالات جديدة، أو الاحتفاظ بها لتلبية الاحتياجات

(116) للاطلاع على أحدث الإرشادات بشأن المتصفحات وغيرها من التدابير الأمنية التشغيلية، انظر the Computer Security Resource Center of the United States National Institute of Standards and Technology (https://csrc.nist.gov).

(117) Techopedia, "Virtual machine (VM)", 21 May 2020. يمكن الاطلاع عليه في الرابط التالي: www.techopedia.com/definition/4805/virtual-machine-vm.

المستقبلية. وبدلاً من ذلك، يمكن للمحققين اتباع نهج أشق، وإن كان فعالاً نسبياً أيضاً، لتغيير ظهورهم يدوياً باستخدام متصفحات مختلفة كلما اتصلوا بالإنترنت وتبديل الإعدادات للحد من تفرد بصمات أجهزتهم واستخدام المكونات الإضافية التي تحول دون التتبع.

3- البنية التحتية الأخرى

103- وحري بالمحققين، قبل البدء في عملهم، أن يفكروا في بنية تحتية أخرى لحماية شبكاتهم وبنيتهم التحتية، بما في ذلك الأنظمة التالية:

(أ) نظام الحفظ الاحتياطي للبيانات؛

(ب) أنظمة تسجيل للتحقق من الأنشطة وتتبع أفعال المستخدم؛

(ج) أنظمة تخزين منفصلة ومواقع تخزين مناسبة لجمع المواد الرقمية التي تم تحديدها أثناء عمليات البحث. ولحماية البيانات من الخارج، ينبغي أن يكون لدى المنظمات منصات (مثل مستودعات الأدلة أو قواعد البيانات أو أنظمة إدارة المعلومات الأخرى) يُحتفظ بها منفصلة عن الشبكات الرئيسية. وينبغي أن تحتوي المنصات على جزأين رئيسيين: أحدهما متصل بالإنترنت والآخر غير متصل بها. وفي بعض الحالات، قد يكون من المناسب إزالة البيانات من البنية التحتية المتصلة بالإنترنت إلى شبكة/مستودع أكثر أمناً في أقرب وقت ممكن، بحيث يمكن استعراض المعلومات بأمان.

دال- الاعتبارات المتعلقة بالمستخدم

104- يُعد المستخدم من أكثر النقاط ضعفاً في أي إطار أمني. وحتى إن وُجدت بنية تحتية مثالية، فلن يتم الالتزام بمبادئ الأمن دون تكييف سلوك المستخدم من خلال التدريب والإشراف المنتظمين. وتقع مسؤولية الأمن على عاتق الجميع. وينبغي ألا ينخرط الأفراد في أنشطة قد تعرِّض البيانات، أو الأشخاص، لأخطار دون أن يتلقوا تدريباً مناسباً على سبل تخفيف حدة تلك الأخطار. وينبغي تدريب المحققين على تقييم السلوك المناسب عند إجراء أنشطة مختلفة عبر الإنترنت.

105- ويمكن أن يساعد إخفاء الهوية في تقليل الضرر إلى أدنى حد في المواقف التي تحاول فيها جهة فاعلة مهدِّدة تتبع أصل النشاط للوصول إلى الشبكة أو المستخدم[118]. وكل نشاط عبر الإنترنت معرَّض للتتبع من قبل أطراف ثالثة. لذلك، ينبغي للمحققين أن يفترضوا وجود هذا التهديد عند إجراء أنشطة عبر الإنترنت. ومن أكثر موضوعات التتبع شيوعاً عناوين بروتوكول الإنترنت والمتصفحات ودقة الشاشة (المستخدمة لتحديد المعدات)، بالإضافة إلى وقت التنقل والنشاط على مواقع شبكية (مثل مصطلحات البحث التي تم إدخالها، أو الصفحات التي تمت زيارتها). وقد تحاول جهة فاعلة مهدِّدة تحديد مصدر النشاط عبر الإنترنت. وإن جرت محاولة لتتبع الأثر، وجب توجيه الجهة الفاعلة المهدِّدة بعيداً عن الموقع الحقيقي، أو هوية المحقق، أو هيئة التحقيق. ويتحقق ذلك باتخاذ تدابير للظهور على الإنترنت وكأن النفاذ إليها يتم من مكان آخر باستخدام شبكة افتراضية خاصة، على سبيل المثال، أو كشخص آخر، بإنشاء هويات افتراضية واستخدامها[119].

106- ويتيح إخفاء الاتصال والجهاز المستخدم فيه في تحقيق عبر الإنترنت مستوى مهماً من الحماية. بيد أنَّ هذه الحماية قد تُقوض إن كشف المستخدمون عن أنفسهم بتحديد هويتهم على موقع شبكي أو قاموا، على سبيل المثال، باستخدام المعلومات الشخصية للتسجيل، أو تسجيل الدخول إلى منصة وسائط اجتماعية، أو حساب خاص آخر. وحري بالمحققين الأَّ يستخدموا مطلقاً حساباتهم الشخصية لأغراض التحقيق، أو تسجيل الدخول إلى الحسابات الشخصية في متصفح يُستخدم للتحقيقات المفتوحة المصدر. وقد تتطلب بعض الحسابات عند إنشائها استخدام الصور الفوتوغرافية، أو أرقام الهواتف، أو البريد الإلكتروني. وينبغي ألا تُستخدم بتاتاً الصور الفوتوغرافية، أو الهواتف، أو رسائل البريد الإلكتروني، أو البيانات الشخصية، أو المنسوبة إلى المحققين، أو إلى غيرهم.

تمويه المستخدم

107- الهوية الافتراضية[120] هي هوية، أو ملف تعريف مزيف عبر الإنترنت، يمكن استخدامه لإجراء أنشطة تحقيق آمنة على منصات التواصل الاجتماعي وغيرها من المنصات المفتوحة على شبكة الإنترنت التي تتطلب من المستخدمين تسجيل الدخول للنفاذ إلى المحتوى. وقد يشمل ذلك أيضاً حساباً افتراضياً، أو خدمة بريد إلكتروني، أو تراسل، أو قاعدة بيانات،

(118) التتبع هو اكتشاف نقطة منشأ شخص ما أو شيء ما بتتبع مسار من المعلومات، أو سلسلة من الأحداث بشكل ارتجاعي.

(119) للاطلاع على مناقشة للهويات الافتراضية، انظر أيضاً الفصل الثاني-جيم، والفصل الثالث-واو، والفصل الرابع-ألف وجيم أعلاه.

(120) ينبغي لأي استخدام للهويات الافتراضية أن يوازن بين الحاجة إلى الأمن والمبدأ الأخلاقي المتمثل في الشفافية. انظر الفصل الثاني-جيم أعلاه بشأن المبادئ الأخلاقية.

أو منتجاً، أو تطبيقاً يستخدم هوية مزيفة عبر الإنترنت بدلاً من هوية الشخص الحقيقية في الحياة. ومن منظور أمني، يجدر بالمحققين المتخصصين في المصادر المفتوحة إنشاء هويات افتراضية لأنشطة التحقيق عبر الإنترنت المتصلة بالمواد المفتوحة المصدر واستخدام هذه الهويات وذلك حتى تجد الجهة الفاعلة المهدِّدة معلومات متسقة ومقنعة تستند إلى الهوية الافتراضية التي لا تكشف النقاب عن معلومات حقيقية عن المحقق أو هيئة التحقيق، أو معلومات عن محتوى التحقيق، أو مجال تركيزه، إن هي حاولت تتبع أنشطة هذا الملف الشخصي عبر الإنترنت. ويمثل ذلك أيضاً إجراءً أمنياً هاماً لحماية الذين يدعمون التحقيق. وينبغي التخطيط للملفات الشخصية والحسابات الافتراضية والأنشطة التي تُستخدم فيها[121]. وينبغي الاحتفاظ بسجلات عن المعلومات المستخدمة في إنشاء الحسابات وتسجيل الأنشطة التي تستخدم هذه الحسابات بحيث يمكن شرحها لاحقاً إن لزم الأمر، على سبيل المثال، في المحكمة[122].

(121) انظر الفصل الخامس-جيم أدناه بشأن خطة التحقيق على الإنترنت.

(122) انظر الفصل السادس-دال أدناه بشأن الحفظ.

خامساً

الإعداد

موجز الفصل

- الإعداد والتخطيط الاستراتيجي هما المفتاح لإجراء تحقيق شامل وآمن.
- يشمل الإعداد ثلاث عمليات هي: (أ) تقييم التهديدات والأخطار ووضع خطة لتخفيف حدتها؛ (ب) تقييم المشهد المعلوماتي؛ (ج) وضع خطة للتحقيق. وقد تتداخل هذه العمليات و/أو تتكرر طوال فترة التحقيق.
- يتضمن الإعداد وضع خطة للتعامل مع أي جوانب نفسية سلبية في التحقيق، مثل تلك التي قد تنجم عن التعرض لمواد صادمة أو مسببة لصدمة نفسية.
- يشمل الإعداد وضع خطة تبيِّن سبل التعامل مع أي معلومات تُجمع طوال مدة الخطة، بما في ذلك متى ينبغي حذف هذه المعلومات وفي أي ظروف وسبل تقاسمها وفي أي الأحوال ومن ينبغي أن يكون له حق النفاذ إليها.
- ينبغي أن يشمل الإعـداد تقييماً للبرمجيات والأدوات الأخرى التي يحتمل أن تكون مفيدة. وحري بالمحققين أن يفهموا أوجه المفاضلة بين الموارد التجارية والمخصصة والمفتوحة المصدر.

108- ينبغي ألا يبدأ المحققون المتخصصون في المصادر المفتوحة أنشطة التحقيق عبر الإنترنت إلا بعد اتخاذ بعض التدابير التحضيرية. ويتوخى في الخطوات التحضيرية أن تشمل إجراء تقييم رقمي للتهديدات والأخطار وتقييم للمشهد الرقمي[123]. وحري بهم أن يضعوا بعد ذلك خططاً للتحقيق عبر الإنترنت، مستعينين في ذلك بالمعلومات المستقاة من تلك التقييمات. ويرد أدناه تفصيل لكل من هذه الأنشطة.

109- وعلى صعيد المنظمة، من المهم أيضاً وضع سياسات للاحتفاظ بالبيانات وحذفها والنفاذ إليها وتبادلها قبل جمع المعلومات وحفظها، على النحو المفصل أدناه.

ألف- تقييم التهديدات والأخطار الرقمية

110- يكفل التفكير في التهديدات المحتملة واعتماد استراتيجية لإدارة الأخطار – سواء أكانت مادية، أو رقمية، أو نفسية – الامتثال للمبادئ الأمنية والأخلاقية. وينبغي، بادئ ذي بدء، إجراء تقييم رقمي للتهديدات والأخطار وتحديد التهديدات العامة والخاصة بكل حالة على حدة التي قد تنشأ نتيجة للأنشطة عبر الإنترنت، ولا سيما زيارة المواقع الإلكترونية المستهدفة، أو إجراء رصد مستمر لمصادر محددة، أو استخراج بيانات من منصات التواصل الاجتماعي. وينبغي أن يشمل التقييم بعض عناصر تحليل التهديدات التقليدي، مثل تحديد جميع الجهات الفاعلة المهدِّدة المحتملة وتقييم مصالح هذه الجهات وقدراتها واحتمال وقوع هجوم ومراعاة مواطن الضعف ووضع تدابير الحماية موضع التنفيذ لتقليل مواطن الضعف تلك إلى أدنى حد. ويُستعان في هذا التقييم بإجراء مشاورات مع خبراء الأمن أو بأفكارهم، ولا سيما من لديه منهم خبرة في مجال الأمن السيبراني[124]. وينبغي استعراض التقييم وتحديثه دورياً، حسب الضرورة. وبالإضافة إلى ذلك، قد يستدعي الأمر إجراء مزيد من التقييمات لمعالجة أنواع محددة من الأنشطة على الإنترنت أو لإدخال جهات فاعلة مُهدِّدة جديدة محتملة[125].

باء- تقييم المشهد الرقمي

111- ينبغي للمحققين المتخصصين في المصادر المفتوحة فهم البيئة الرقمية الخاصة بالوضع قيد التحقيق. وسيكون لنوع التكنولوجيا المتاحة والمستخدمة والجهة التي تستخدمها تأثير في أنواع البيانات الرقمية المتاحة، وهو أمر يتطلب تحديد أكثر المنصات استخداماً على الإنترنت وخدمات الاتصالات ومنصات وسائط التواصل الاجتماعي والتقنيات النقالة والتطبيقات النقالة المستخدمة في المنطقة الجغرافية قيد التحقيق. فعلى سبيل المثال، سيكون على المحققين في التحقيقات المتعلقة بجرائم الحرب معرفة أنواع وسائل النقل وتكنولوجيا المعلومات والاتصالات والوسائط الرقمية التي تستخدمها جميع الأطراف المشاركة في النزاع المسلح، فضلاً عن غير المشاركين فيه، أو الشهود الآخرين، وذلك لمعرفة أنواع المعلومات التي يُرجح التقاطها وتوزيعها عبر الإنترنت.

112- وينبغي للمحققين أن يدرسوا فئات المستخدمين لكل تلك التكنولوجيات أو من يمكنهم النفاذ إليها في تلك المنطقة الجغرافية. وفي هذا الصدد، ينبغي أن يدرك المحققون أنَّ المحتوى الرقمي المتاح للجمهور الذي ينشئه المستخدمون، بما في ذلك المنشورات في وسائل التواصل الاجتماعي والمعلومات المتبادلة عبر المنصات الشبكية، قد لا يشمل، بشكل كامل ومتساو، نطاق الانتهاكات المرتكبة ضد جميع الأفراد والجماعات. وذلك لأنَّ استخدام التكنولوجيات الرقمية قد يختلف لأسباب عديدة من بينها نوع الجنس[126] والعرق والدين والمعتقد والعمر والوضع الاجتماعي والاقتصادي والانتماء إلى أقلية عرقية، أو لغوية، أو دينية[127] وهوية

(123) انظر أدناه، المرفق الثاني بشأن نموذج تقييم التهديدات والأخطار الرقمية، والمرفق الثالث بشأن نموذج تقييم المشهد الرقمي.

(124) للاطلاع على معلومات عامة عن التهديدات والأخطار في التحقيقات المفتوحة المصدر، انظر الفصل الرابع أعلاه بشأن الأمن.

(125) انظر المرفق الثاني أدناه بشأن نموذج تقييم التهديدات والأخطار الرقمية.

(126) على سبيل المثال، قد لا تتمكن النساء والفتيات والمثليات والمثليون ومزدوجو الميل الجنسي ومغايرو الهوية الجنسانية وحاملو صفات الجنسين من استخدام الهاتف المحمول العائلي أو الحصول عليه. وللاطلاع على مزيد من النقاش بشأن ما يسمى "الفجوة الرقمية بين الجنسين"، انظر A/HRC/35/9. انظر أيضاً Human Rights Council resolution 32/13, and Araba Sey and Nancy Hafkin, eds., *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership* (Macao, China, EQUALS Global Partnership and the United Nations University, 2019). يمكن الاطلاع عليه في الرابط التالي: www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf.

(127) على سبيل المثال، قد يواجه من ينتمون إلى أقليات لغوية حواجز في النفاذ إلى فضاء الإنترنت الذي يدار عادة باللغة السائدة. بيد أنَّ بعض الأقليات اللغوية قد يكون لديها أيضاً فضاء يخصها على الإنترنت تديره بلغاتها أو تستخدم هذه اللغات فيه. ولذلك، قد يحتاج المحققون إلى البحث باستخدام لغات الأقليات (ومن بينها لغات الشعوب الأصلية).

السكان الأصليين ووضع الهجرة والموقع الجغرافي[128]. وقد يكون هذا الاختلال ناتجاً عن العجز عن الوصول إلى الأجهزة، أو المرافق، أو الموارد بحيث لا تُتاح لهؤلاء الأفراد الفرصة لإنشاء معلومات على الإنترنت عن المسائل والانتهاكات المتعلقة بهم، أو تحميلها[129]. وثمة عامل آخر يتمثل في أنَّ المذكورين أعلاه ربما تعذر عليهم، من بين أمور أخرى، الحصول على قدر متساوٍ من التعليم وبالتالي تكون قدراتهم من حيث المهارات التقنية أقل. ونتيجة لأشكال التمييز المتداخلة، قد تكون شرائح معينة من المجتمع غير مرئية بشكل مضاعف على الإنترنت، فعلى سبيل المثال، قد تكون المعلومات عن النساء والفتيات المنتميات إلى إحدى الفئات المهمشة المذكورة أعلاه أقل تمثيلاً في المعلومات المفتوحة المصدر. وتعني هذه العوامل أنَّ هؤلاء الأشخاص لن يكونوا من ينشئون المحتوى أو موضوعاً له، مما يشوه نتائج أي تحقيق عبر الإنترنت.

113- وعلاوة على ذلك، فإن انعدام المساواة في استخدام جميع شرائح المجتمع للتكنولوجيا قد يشوش أيضاً التركيز على من يمثله المحتوى المنشور على الإنترنت، بل وأنواع الانتهاكات المتاحة عليها، ولا سيما المحتوى الذي ينشئه المستخدمون. فعلى سبيل المثال، عندما تتشارك النساء في استخدام هواتف محمولة يملكها الذكور من أفراد أسرهن، أو يتشاركن في حساب مع آخرين، فإنَّهن قد يعزفن عن مناقشة قضايا حساسة، مثل العنف الجنسي والجنساني، أو مسائل الصحة الجنسية والإنجابية. وعلاوة على ذلك، قد يصوِّر المحتوى الذي ينشئه المستخدمون على وسائل التواصل الاجتماعي، بما في ذلك الصور الفوتوغرافية ومقاطع الفيديو، انتهاكات بعينها بسهولة أكبر من غيرها، فعلى سبيل المثال، قد يكون تصوير العنف الجنسي والجنساني الذي يرتكب في أماكن خاصة أصعب من التقاط صور لعمليات الإخلاء.

114- ولئن كان تخفيف وقع بعض هذه العوامل مستطاعاً بالسعي إلى النفاذ إلى عدد كبير من أنواع المعلومات المنشورة على الإنترنت وعدم الاكتفاء بالمحتوى الذي ينشئه المستخدمون، فإنَّ هذه العوامل ذاتها ينبغي أن تؤخذ في الحسبان عند تحليل أنواع أخرى من المعلومات المفتوحة المصدر. فعلى سبيل المثال، عند النفاذ إلى بيانات وإحصاءات تضعها الحكومة، ينبغي للمحققين أن يتساءلوا على الدوام إن كانت هذه البيانات تستوعب بدقة جميع شرائح المجتمع وجوانبه[130]. وثمة مسائل وتكنولوجيات رئيسية عديدة يمكن تقييمها استناداً إلى ما يكون منها وثيق الصلة بتحقيق بعينه ونطاق هذا التحقيق الجغرافي والزمني. وينبغي للمحققين أن يراعوا نوع الجنس والعمر والجغرافيا وأوجه التفاوت الاجتماعي والاقتصادي وغيرها من المعلومات الديمغرافية ذات الصلة. ويكمن الهدف المنشود من وراء هذا التقييم في أن يفهم المحققون الحالات قيد التحقيق فهماً أفضل يمكِّنهم من وضع استراتيجيات تحقيق فعالة عبر الإنترنت ويحملهم على النظر مسبقاً في أوجه التحيز المحتملة في البيانات المتاحة عبر الإنترنت. وقد لا تكون جميع هذه الفئات ذات صلة بجميع التحقيقات. ولذلك، يجب على المحققين تكييف تقييم المشهد الرقمي ليتناسب مع الحالة التي تخصهم[131]. وللاطلاع على قائمة كاملة بفئات المعلومات التي يمكن إدراجها في تقييم المشهد الرقمي، انظر المرفق الثالث أدناه.

جيم- خطة التحقيق عبر الإنترنت

115- قبل الشروع في إجراء تحقيق مفتوح المصدر، ينبغي وضع خطة تحقيق عبر الإنترنت[132] تشمل ما يلي: (أ) استراتيجية التحقيق الشاملة؛ (ب) أنشطة تحقيق محددة عبر الإنترنت. وإن كانت التحقيقات عبر الإنترنت جزءاً من تحقيق أوسع نطاقاً تُستخدم فيه التقنيات التقليدية، مثل أخذ أقوال الشهود، أو جمع الأدلة المادية، فينبغي دمج خطة التحقيق عبر الإنترنت في خطة التحقيق الرئيسية. ويجدر بالمحققين أن يدرجوا في خطة التحقيق منظوراً جنسانياً لكي يشمل التحقيق جميع الشواغل الجنسانية ويأخذ في الحسبان التباين في الوصول إلى التكنولوجيا[133]. ويتوخى في خطة التحقيق عبر الإنترنت أن تتناول المواضيع التالية.

(128) على سبيل المثال، قد تكون إمكانية الاتصال بالإنترنت أضعف في المناطق الريفية.

(129) مثل عدم الحصول الفعلي على اتصال إنترنت سريع، أو العجز عن شراء الأجهزة، أو دفع رسوم الاشتراك.

(130) انظر، بصفة عامة، المفوضية السامية لحقوق الإنسان، نهج *قائم على حقوق الإنسان إزاء البيانات، عدم إغفال أي أحد في خطة التنمية المستدامة لعام 2030* (جنيف، 2018). يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData_AR.pdf.

(131) للاطلاع على النموذج، انظر المرفق الثالث أدناه.

(132) انظر المرفق الأول أدناه بشأن نموذج خطة التحقيق عبر الإنترنت.

(133) للاطلاع على مزيد من الارشادات بشأن كيفية دمج منظور جنساني، انظر: *إدماج المنظور الجنساني في التحقيقات المتعلقة بحقوق الإنسان: توجيهات وممارسات* (نيويورك وجنيف، 2019) (United Nations publication, Sales No. 19.XIV.2).

1- الأهداف والأنشطة المقررة

116- ينبغي أن تحدد الخطة أهداف التحقيق المفتوح المصدر وأولوياته والاستراتيجية المقترحة لتحقيق هذه الأهداف وجدولاً زمنياً لتنفيذها.

2- استراتيجية إدارة الأخطار

117- ينبغي أن تتضمن الخطة النتائج الرئيسية لتقييم التهديدات والأخطار الرقمية المذكورة أعلاه، مثل التهديدات السيبرانية المحتملة، إلى جانب استراتيجية لإدارة الأخطار، بما في ذلك سبل تحديد الخروقات، أو الهجمات، والتصدي لها والتعافي منها.

3- حصر الجهات الفاعلة وفرص التعاون

118- قد يرى المحققون المتخصصون في المصادر المفتوحة حصر الجهات الفاعلة الأخرى التي تجري تحقيقات مماثلة أو متداخلة لتقييم إمكانية تأثير أنشطتها بعضها في بعض واستكشاف فرص عقد الشراكات والتعاون المحتملة. ويشمل ذلك تحديد أمناء المحفوظات الرقمية، أو الصحفيين، أو المجموعات الأخرى، أو الأفراد الآخرين الذين يحتفظون بمحتوى منشور على الإنترنت قد تكون له صلة بالتحقيق. وينبغي أن يُراعى في هذا الحصر أيضاً التحيز المحتمل والقيود المفروضة على الجهات الفاعلة الأخرى التي قد تؤدي إلى استنتاجات تتوصل إليها أطراف ثالثة لا تستوعب تماماً التعقيدات التي تتسم بها حالة بعينها، أو تستبعد مجموعات معينة بسبب التحيز المتأصل في المجال الرقمي الذي لم يؤخذ في الحسبان على النحو الموضح أعلاه. وإن انعقدت هذه الشراكات، سيكون من المفيد إبرام اتفاق مكتوب لتبادل المعلومات.

4- الموارد

119- ينبغي أن تحدد الخطة الموارد اللازمة لتنفيذ الأنشطة المقررة، ويشمل ذلك التوظيف والتدريب والأدوات والمعدات. ويتوخى في تقييم الاحتياجات من الموظفين أن يشمل عدد أعضاء الفريق اللازمين للاضطلاع بالمهام وكفاءاتهم وشمول أعضاء الفريق وتنوعهم وتقييم الاحتياجات من التدريب الإضافي. ويشمل ذلك إجراء تقييم للبنية التحتية الضرورية التي تشمل الأجهزة والبرمجيات والتكاليف المالية للحفاظ على المواد الرقمية في الأجل الطويل. وينبغي أن تكفل الخطة أيضاً وجود موارد مكرسة لتضمن للمحققين الرفاه النفسي الذي يراعي الفوارق بين الجنسين، ولا سيما في الحالات التي يتناول فيها التحقيق المفتوح المصدر محتوى صادماً، أو يكون فيها المحققون، أو الأطراف الثالثة المشاركة في التحقيق، عرضة بشكل خاص للانتقام إن أُفشيت هوياتهم أو خصوصيتهم[134].

5- الأدوار والمسؤوليات

120- عند العمل في إطار فريق، أو مع شركاء خارجيين، ينبغي تحديد أدوار المحققين المتخصصين في المصادر المفتوحة ومسؤولياتهم تحديداً جيداً، مع مراعاة الحاجة إلى تنسيق الأنشطة تنسيقاً يحول دون الازدواجية فيها وفي جمع البيانات. وفضلاً عن ذلك، ينبغي أن ينظر هذا الفرع من الخطة في مجالات الخبرة المتخصصة التي يستلزمها التحقيق المعني وفي حاجة المحققين إلى استشارة خبير أو الاستعانة به حين لا يتضمن الفريق القائم خبيراً. وتشمل مجالات الخبرة المتخصصة الأدلة الجنائية الرقمية وتحليل صور الأقمار الصناعية وعلوم البيانات. وفي بعض مجالات الخبرة، قد يلزم بذل جهود استباقية لتحديد الخبراء من مختلف الخلفيات الجنسانية وسواها من الخلفيات، حرصاً على أن يكون فريق التحقيق شاملاً ومتنوعاً شأنه في ذلك شأن التحليل الذي يجريه.

6- التوثيق

121- ينبغي توثيق التحقيقات المفتوحة المصدر باتباع طريقة توثيق تتيح إدارة التحقيقات بكفاءة والامتثال لمبدأ المساءلة. وعند اتخاذ إجراءات قانونية، ينبغي أن تمكِّن هذه الوثائق المحققين من إثبات جدوى الأدلة التي جُمعت وقيمتها الإثباتية وشرح الخطوات المتخذة، أو غير المتخذة، أثناء سير الأنشطة عبر الإنترنت والسبب وراء ذلك. وينبغي أن تكون في النظام، سواء أكان ذلك بتكليف ذاتي، أو من قبل مشرف، آلية لوضع مهام لأنشطة تحقيق بعينها، بما في ذلك الأنشطة عبر الإنترنت، مثل طلبات إجراء بحث يتناول شخصاً بعينه، أو غير ذلك من عمليات الاستقصاء. وينبغي أن تشير النتائج التي تحققها المهام، ومن بينها التقارير، إلى المنهجيات والتقنيات المستخدمة. ويتوخى في الإبلاغ أن يميِّز بين المعلومات التشغيلية التي ينبغي الحفاظ على

(134) على سبيل المثال، قد يواجه المحققون خطاب كراهية أو مضايقة عبر الإنترنت وقد تكون هذه الهجمات جنسانية (على سبيل المثال، قد يكون المحققون من النساء والمثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسانية وأحرار الهوية الجنسانية وحاملي صفات الجنسين أكثر عرضة من المتوسط لخطاب الكراهية والتشهير وتهديدات الاغتصاب عبر الإنترنت وغيرها من التهديدات العنيفة ذات الطبيعة الجنسية أو الجنسانية). انظر، على سبيل المثال، Amnesty International, "Toxic Twitter - a toxic place for women". يمكن الاطلاع عليه في الرابط التالي: www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

سريتها لحماية مصادر التحقيق وأساليبه ومعلومات التحقيق التي يجب الكشف عنها أثناء الإجراءات القانونية.

122- وينبغي استعراض خطة التحقيق عبر الإنترنت بانتظام وتعديلها، حسب الاقتضاء. انظر المرفق الأول أدناه للاطلاع على نموذج خطة التحقيق على الإنترنت.

دال- خطة القدرة هعلى التحمل والرعاية الذاتية

123- قد لا يُجري المحققون المتخصصون في المصادر المفتوحة مقابلات شخصية أو يزورون مسرح الجريمة بأنفسهم، إلا إنَّ خصوصيات البحث الرقمي تعني أنهم قد يتعرضون لمشاهدة وجمع وتحليل كميات كبيرة من المعلومات الرقمية الصادمة، أو غير ذلك من المعلومات الصادمة نفسياً، التي قد تحدث، في ما تحدثه، صدمة ثانوية. وحري بالمحققين المتخصصين في المصادر المفتوحة أن يكونوا على دراية بمبادئ الرعاية الذاتية[135]. وينبغي لمديري التحقيقات أن يهيئوا بيئة تنظيمية تُعنى بالرعاية الذاتية وبالحساسية الجنسانية والثقافية. ويحبذ أن يكون ذلك في المرحلة التحضيرية من التحقيق، بإعداد خطة لتعزيز القدرة على التحمل وتخفيف آثار التحقيق السلبية النفسية التي قد تتفاوت وطأتها تبعاً لنوع الجنس والثقافة والعمر. وتُعد هذه الخطة ضرورية لأسباب أخلاقية بحسبانها جزءاً من عملية تعزيز واحترام حقوق الإنسان الخاصة بكل عضو في فريق التحقيق. وهذه الخطة ضرورية أيضاً لتحقيق أقصى قدر من الأمن المادي والرقمي. ويُعد الشخص المجهد نفسياً نقطة ضعف تهدد سلامة الفريق وأمن المعلومات وتقلل من جودة العمل، حتى وإن كان هذا الشخص قد تلقى تدريباً مناسباً. ويجدر تخصيص وقت وموارد مكرسة لهذا الغرض تتيح تنفيذ الخطة التنفيذ السليم، لا سيما حين يُتوقع أن يتضمَّن التحقيق عبر الإنترنت مشاهدة كم هائل من الصور الصادمة تشمل محتوى عنيفاً أو مثيراً للإزعاج بوجه آخر. وتتنوع استراتيجيات تخفيف التأثير السلبي الذي قد تحدثه مشاهدة محتوى صادم ولكنها تندرج بوجه عام في ثلاث فئات هي: الوعي الفردي وأساليب تقليل التعرض والدعم المجتمعي.

124- أولاً، يجدر بالمحققين أن يكونوا على دراية بأنماط سلوكهم وسلوك زملائهم في الفريق الأساسية، بما في ذلك أنماط العمل والترفيه والنوم والأكل، حتى يتسنى اكتشاف الانحرافات ومعالجتها. ويمكن أن يساعد وجود سياسة تقضي بأن يعمل المحققون أزواجاً في الكشف عن الانحرافات لأنَّ الأفراد ربما لا يدركون حدوث تغييرات في سلوكهم قد يلاحظها الآخرون بسهولة أكبر، أو لا يرغبون في ذلك. ويُتوقع من أعضاء الفريق أن يراعوا ويحترموا الاختلافات في ردود الفعل حيال المواد الصادمة وغيرها من المواد التي قد تثير عاطفة جياشة وأن يدركوا أنَّ هذه الاختلافات قد تتفاوت بين الأفراد والأجناس والمجموعات الثقافية وتتباين مع مرور الوقت في حالة أفراد بعينهم بسبب درجة الضغط التي يتعرضون لها والعوامل الظرفية الأخرى. ويُنتظر من المحققين أيضاً أن يدركوا أنَّ رد الفعل العاطفي حيال محتوى صادم، أو فاضح، أمر طبيعي جداً في غالب الأحيان وليس دلالة على الضعف، بل قد يكون دالاً على تصرف صحي - إن لم نقل على القوة.

125- ثانياً، ينبغي اعتماد أساليب تتيح تقليل التعرض للمحتوى الضار إلى الحد الأدنى. وتشمل الاستراتيجيات الشائعة في هذا الصدد إيقاف تشغيل الصوت عند مشاهدة محتوى صادم لأول مرة، أو عندما لا يكون ذلك ضرورياً لمهمة التحليل الفورية، وذلك لأنَّ قسطاً وافراً من المحتوى العاطفي مضمَّن في الصوت؛ وتقليل حجم الشاشات إلى أقصى حد ممكن وتغطية المواد الصادمة عند تحليل السياق المحيط بفعل معين وليس الفعل نفسه ووضع علامة على أي محتوى صادم في مجموعة بيانات حتى لا يشاهده الأفراد دون علم مسبق بما يوشكون على مشاهدته ويتمكنوا من تنبيه بعضهم بعضاً عند تبادل المحتوى الصادم، تخفيفاً لعنصر المفاجأة، والعمل في أزواج وتجنب العمل العمل في عزلة، أو في وقت متأخر من الليل، وأخذ فترات راحة منتظمة، حسب الاقتضاء.

126- ثالثاً، ينبغي على الأفراد والمنظمات أن يبثوا بين أفراد الفريق الشعور بالانتماء إلى جماعة، وهو أمر يؤمل أن يكون له تأثير وقائي يتمثل أساساً في إحياء روح الرفقة التي تنشأ عند إجراء التحقيقات في الميدان. ويمكن تحقيق ذلك بتقديم إحاطات بالمعلومات بانتظام للحد من العزلة ومساعدة المحققين على فهم آثار عملهم الإيجابية فهماً أفضل وأنشطة الفريق الترفيهية، ومن بينها الاحتفال بمراحل التحقيق الهامة؛ وتدريب الفريق على استراتيجيات التحمل. وتكون محاولات زيادة القدرة على التحمل مؤثرة بشكل خاص عندما تتناول المستويات الفردية والثقافية والهيكلية، على سبيل المثال بتمكين الأفراد من التفكير النقدي في احتياجاتهم النفسية والاجتماعية عند العمل في تحقيق وتهيئة بيئة تُحملُ فيها جوانب العمل النفسية والاجتماعية محمل الجد وتُشجع الممارسات الداعمة صراحة وضمناً ويُعتمد مبدأ الشمول والتنوع.

(135) لمزيد من النقاش بشأن أهمية الرعاية الذاتية للعاملين في مجال التحقيقات في حقوق الإنسان، انظر OHCHR, *Manual on Human Rights Monitoring* (Geneva, 2011), chap. 12 on trauma and self-care, pp. 20-39. يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf.

هاء- سياسات البيانات وأدواتها

127- ينبغي وضع سياسات لمعالجة البيانات وحفظها وإتلافها وتنفيذ هذه السياسات والتقيد بها أثناء التحقيق. وينبغي للمؤسسات أن تضع سياسات لحفظ المعلومات (سياسات الاحتفاظ) وحذف المعلومات (سياسات الحذف)، عند الاقتضاء، فضلاً عن سياسات النفاذ إلى المعلومات (داخلياً) وتبادل المعلومات (خارجياً). وبالإضافة إلى ذلك، قد يكون من المفيد وضع سياسات محددة لإنشاء الهويات الافتراضية واستخدامها، فضلاً عن النفاذ إلى البرامج المعتمدة والأدوات المستخدمة.

1- سياسات البيانات

(أ) سياسات الاحتفاظ بالبيانات

128- تُعد سياسات الاحتفاظ بالبيانات مهمة للامتثال للعديد من قوانين حماية البيانات وأنظمة الاحتفاظ بالبيانات. وفي بعض الحالات، يوجد حد أدنى من المتطلبات بشأن المدة التي يجب الاحتفاظ فيها بالبيانات وحد أقصى لهذه المدة في ظروف أخرى. وينبغي أن تحدد السياسات النُهج المتبعة في تخزين البيانات المطردة وإدارة السجلات، نشداناً للوفاء بالمتطلبات القانونية ومتطلبات حفظ البيانات التجارية. وتوازن سياسات الاحتفاظ بالبيانات المختلفة بين الشواغل القانونية والمتعلقة بالخصوصية والشواغل الاقتصادية والمتصلة بالحاجة إلى المعرفة لتحديد مُدد الاحتفاظ بالبيانات وقواعد الأرشفة وأنساق البيانات ووسائل التخزين والنفاذ والتشفير المأذون بها[136]. ويلزم فهم القواعد المطبقة لإعداد هذه السياسات.

(ب) سياسات حذف البيانات

129- قد يثير حذف أجزاء من مجموعة بيانات في غياب سياسات حذف واحتفاظ واضحة وبدون سجلات تبيِّن ما حُذف ومن حذفه ومتى حُذف - ولأي أغراض - مشاكل جسيمة، ولا سيما عند استخدام المعلومات في المحاكم. وينبغي على المحققين الامتثال لأنظمة حذف البيانات الرقمية المعمول بها وأن يدركوا أنَّ استخدام طريقة أو أخرى قد يثير مسائل قانونية.

(ج) سياسات النفاذ إلى البيانات

130- يُنتظر أن يكون لدى المؤسسات التي تجمع البيانات وتعالجها، وخاصة البيانات الحساسة، سياسة واضحة تحدد من يمكنهم النفاذ إلى أنواع مختلفة من البيانات. وينبغي وضع أي ترتيبات داخل قواعد البيانات أو الأنظمة بشكل يعبر عن هذه السياسة.

(د) سياسات مشاركة البيانات

131- حري بالمؤسسات أن تنظر في وضع سياسة لمشاركة البيانات مع الجهات الفاعلة الخارجية. وعند العمل مع شركاء خارجيين، ينبغي إعداد مذكرات تفاهم، أو عقود، لضمان امتثال الشركاء لهذه السياسات.

2- إدارة المعلومات

132- قبل الشروع في إجراء تحقيقات مفتوحة المصدر، وخاصة عند البدء في جمع المواد الرقمية وحفظها، ينبغي على المحققين والفرق والمنظمات إنشاء نظام لإدارة المعلومات. وهناك طائفة من الخيارات بشأن هذا النظام. ولا يحبذ البروتوكول اختيار نظام بعينه، بل يعرض في ما يلي الوظائف الرئيسية المفيدة لعملية التحقيق - والمطلوبة في بعض السياقات. وبالإضافة إلى ذلك، ينبغي وضع هياكل أساسية وبروتوكولات للأمن، على النحو المبيَّن في الفصل الرابع.

(أ) نظام إدارة التحقيقات

133- نظام إدارة التحقيقات هو نظام لتوثيق الأنشطة المضطلع بها أثناء التحقيق. وليس لدى جميع المنظمات التي تجري تحقيقات أنظمة من هذا القبيل ولكن يوصى بها بشدة، لا سيما في حالة المنظمات، أو فرق التحقيق الكبيرة. ويمكن استخدام هذه النظم لإسناد المهام والإبلاغ عن الأنشطة على نحو يجعل العملية منهجية وفعالة قدر الإمكان بالحد من ازدواجية الجهود.

(ب) نظم إدارة المعلومات والأدلة

134- تُستخدم نُظم إدارة المعلومات لتخزين البيانات التي تُجمع كجزء من التحقيقات. ويُتوخى في نظام إدارة المعلومات أن يكون قادراً على أداء وظيفتين متمايزتين هما: (أ) تتبع جمع المواد وتناولها؛ (ب) فصل المواد التي يمكن استخدامها كدليل.

3- البنية التحتية - الاعتبارات اللوجستية والأمنية

135- ثمة اعتبارات لوجستية وأمنية مهمة عديدة سواء أتعلق الأمر بتصميم البنية التحتية لمنظمة تجري تحقيقات مفتوحة المصدر أو لتحديد الأدوات التي يحبذ أن يستخدمها محقق مستقل.

(136) Yvonne Ng, "How to preserve open source information effectively", in *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020), pp. 143-164.

وبوجه عام، توجد ثلاثة نُهج لإعداد النظم هي: (أ) إعداد نظم وأدوات بمواصفات معينة؛ (ب) استخدام أدوات وبرمجيات مفتوحة المصدر، أو حرة، متاحة على شبكة الإنترنت؛ (ج) شراء المنتجات التجارية من أطراف ثالثة. ولكلٍ من هذه النهج مزاياه وعيوبه ويعتمد نجاحها على الظروف المحددة والسياق المعيَّن الذي يعمل فيه المحققون. وهنا أيضاً، لا ينادي البروتوكول باتباع نهج دون آخر، بل يعرض مزايا كل نهج وعيوبه، فضلاً عن عوامل محددة ينبغي أخذها في الحسبان عند اتخاذ قرارات بشأن المنتجات المراد استخدامها.

(أ) المنتجات التجارية

136- تتمثل فائدة المنتجات التجارية في أنَّ الأعمال التجارية الخاصة قد يكون لديها بنية تحتية أمنية أفضل وتتمتع بالقدرة على توفير الدعم التقني المستمر والمتسق. غير أنَّ التكاليف تمثل جانباً سلبياً واضحاً في المنتجات التجارية. ثم إنَّ التفاعل مع أطراف ثالثة والتعويل عليها قد يثيران مشكلة للمنظمات التي تحاول الحفاظ على سرية تحقيقاتها. وتحتوي العديد من المنتجات التجارية على شفرة مغلقة المصدر لحماية ملكيتها الفكرية. وقد تثير المنتجات التجارية أيضاً شواغل بشأن ملكية البيانات وقابلية نقلها وتصديرها وتشغيلها بينياً مع النظم الأخرى. أضف إلى ذلك أنَّ الشركات قد ترضخ للضغوط الحكومية للنفاذ إلى المعلومات الخاصة. ومن الشواغل الرئيسية في هذا الصدد أن الشركات حتى وإن كانت لديها فرق أمنية تكفل حماية منتجاتها ومستخدميها، فلا مناص للمستخدمين من أن يثقوا في أن هذه الشركات قد صممت نظمها وستحافظ عليها بصورة سليمة وأنهم لن يتكبدوا تكاليف خفية في مرحلة لاحقة.

(ب) الأدوات المصممة خصيصاً أو المخصصة

137- تتمثل فائدة إعداد أداة مخصصة كلياً، أو تخصيص أداة موجودة أصلاً، في أنَّ المحققين، أو المنظمات، يحتفظون بالسيطرة على النظام بأكمله وعلى بياناتهم ويمكنهم بالتالي تجنب التواصل مع أطراف ثالثة. ويمكن أيضاً دمج الأنظمة المصممة خصيصاً مع الأنظمة الأخرى المخصصة. أما الجانب السلبي، فيكمن في ما يستلزمه وضع هذه النظم وتوفير الدعم لها من وقت وتكلفة وخبرة، وهو أمر يصعب على معظم المنظمات تحقيقه. وفوق ذلك، يصعب، في نظام مغلق مع عدد محدود ممن يجرون اختبارات بيتا وقلة من المستخدمين، تحديد مواطن الضعف، أو الحصول على تعقيبات كافية لتحقيق الأداء الوظيفي الأمثل.

(ج) الأدوات المفتوحة المصدر والمجانية

138- أدوات المصدر المفتوح هي الأدوات التي نشر من أعدوها علناً شفراتها المصدرية بحيث يمكن لأي شخص استخدامها أو تعديلها بحرية. وتوجد منتجات تجارية مشفوعة بشفرات مصدرية مفتوحة وأدوات مجانية مصحوبة بشفرات مصدرية مغلقة. بيد أنَّ هذه الحالات استثنائية. والشائع أن تكون الأدوات المفتوحة المصدر مجانية. وتمثل الأدوات المجانية بـديلاً مهماً ينبغي للمؤسسات الصغيرة ذات الميزانيات المحدودة والمنظمات الكبيرة التي تتبع إجـراءات معقدة لشراء المنتجات المدفوعة الأجر مراعاته. بيد أنَّ الأدوات المتاحة مجاناً للمستخدمين تحقق ربحاً بطرق أخرى، مثل بيع بيانات المستخدم والتحليلات بشكل يثير مشكلات بشأن الأمن والخصوصية. زد على ذلك أنَّ استخدام هذه الأدوات يستلزم إجراء بحث مسبق لمعرفة الجهة التي أنشأتها ومدى خضوعها لتدقيق مستقل وإمكانية استدامتها. ويمكن أن تقوض الجوانب الثلاثة هذه مصداقية التحقيق. وعلى وجه الخصوص، تكون الأدوات إشكالية في السياق القانوني إن قُدمت قضية إلى المحاكمة وطَعن الخصم في إحدى الأدوات. ثم أنَّ هذه الأدوات والبرمجيات تستلزم وضع خطة احتياطية ونظام لترحيل البيانات ونظام لحفظها على سبيل الاحتياط إن هي أصبحت مهجورة، أو غدت الجهة التي أعدتها غير متاحة. ومع أنَّ الأدوات المفتوحة المصدر قد تحظى بجاذبية لدى المنظمات لأسباب من بينها استخدام مجموعات أخرى متشابهة في التفكير لها، فإنَّ على المحققين إجراء تقييمات كاملة ومستقلة لكيفية عمل هذه الأدوات وما ينطوي عليه استخدامها من تبعات في سياق بعينه.

139- وعند اتخاذ قرار بشأن المفاضلة بين إعداد أداة حسب الطلب أو استخدام برمجيات تجريبية مجانية أو مفتوحة المصدر، أو شراء منتج، يجدر بالمحققين أن يتبعوا إرشادات العناية الواجبة الواردة في المرفق الخامس أدناه.

سادساً

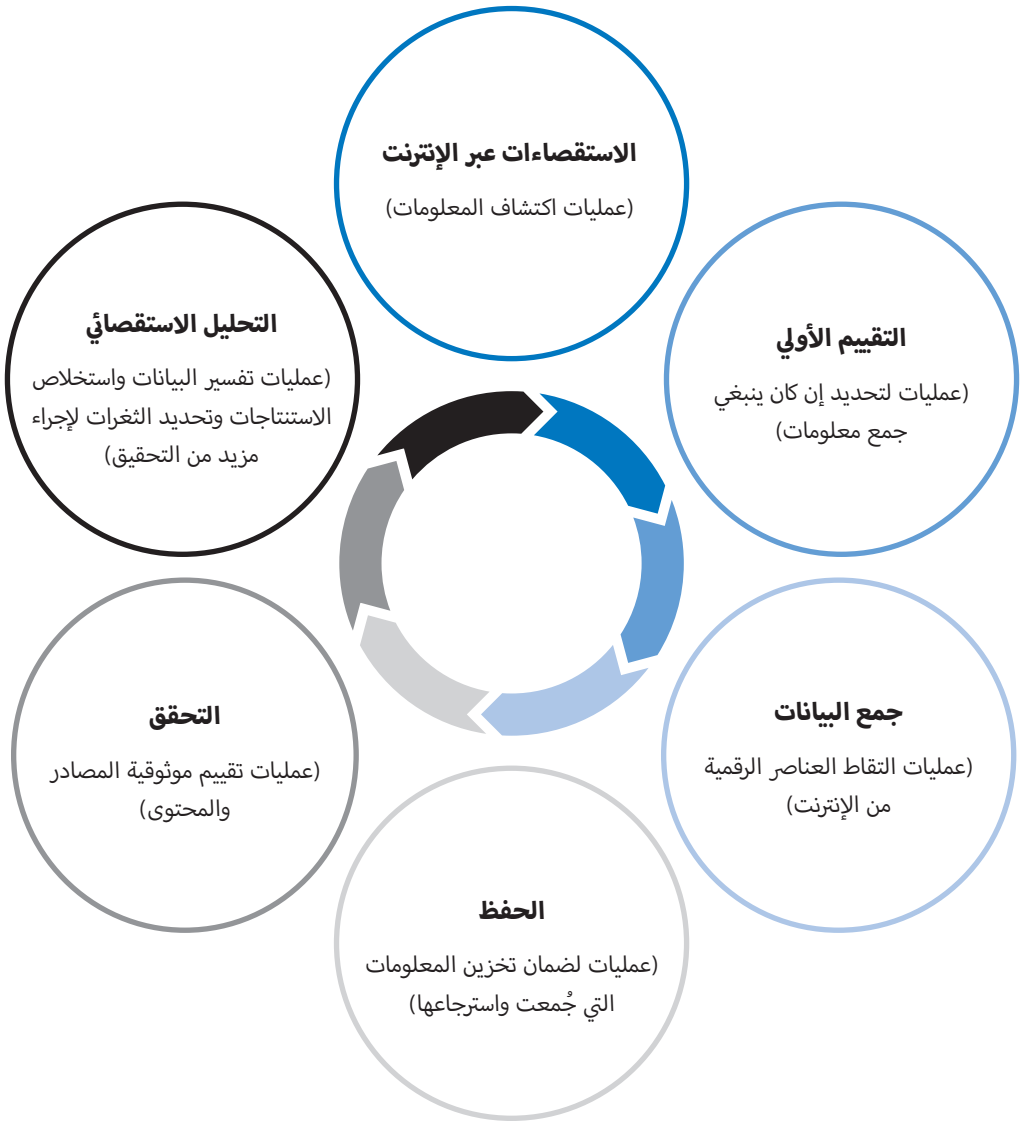
عملية التحقيق

موجز الفصل

- تتألف عملية التحقيق من ست مراحل رئيسية هي: (أ) التحري عبر الإنترنت؛ (ب) التقييم الأولي؛ (ج) جمع البيانات؛ (د) الحفظ؛ (هـ) التحقق؛ (و) التحليل الاستقصائي. وتشكّل هذه العوامل مجتمعة جزءاً من دورة يمكن تكرارها عدة مرات طوال فترة التحقيق، كلما تمخضت المعلومات المكتشفة حديثاً عن مسارات جديدة في سير الاستقصاء.
- ينبغي للمحققين توثيق أنشطتهم خلال كل مرحلة، لأنَّ ذلك سيساعد في فهم تحقيقاتهم وفي شفافيتها، بما في ذلك سلسلة المسؤولية، وفي كفاءة هذه التحقيقات وفعاليتها ويشمل ذلك اكتمالها وفي التواصل بين أعضاء الفريق.

140- تستلزم التحقيقات المفتوحة المصدر مراقبة دقيقة وإجراء استقصاءات منهجية لإثبات الحقائق في بيئة رقمية معقدة وديناميكية. ويجب على المحققين المتخصصين في المصادر المفتوحة النظر نظرة ناقدة في تقييم المحتوى المنشور على الإنترنت وأن تكون لديهم القدرة على تقييم السبل المتبعة في تشويه المواد الرقمية أو المساس بها. وحري بهم أيضاً أن يتبعوا نهجاً متسقاً في الاستقصاء على الإنترنت، مع مراعاة التحيز الخوارزمي وعدم المساواة في توافر المعلومات المفتوحة المصدر المتعلقة بمجموعات محددة والطبيعة الديناميكية التي تتسم بها المعلومات المنشورة عبر الإنترنت. وينبغي دراسة كل واقعة مزعومة بدقة. ويقدم هذا الفصل نهجاً متسقاً للتحقيقات المفتوحة المصدر. ويصوِّر الشكل أدناه دورة التحقيق المفتوح المصدر. ومن المهم أن يُلاحظ أنَّ التحقيقات المفتوحة المصدر قلَّما تكون خطية وغالباً ما تقتضي تكرار هذه العملية نظراً للطبيعة الدورية التي يتسم بها إعداد القضايا. وقد تكون هناك أيضاً أسباب وجيهة لمخالفة هذا التسلسل.

دورة التحقيق المفتوح المصدر



ألف- الاستقصاءات عبر الإنترنت

141- تتألف الاستقصاءات عبر الإنترنت من عمليتين رئيسيتين هما: (أ) البحث، أي اكتشاف المعلومات ومصادرها باستخدام منهجيات البحث العامة أو المتقدمة؛ (ب) الرصد، أي اكتشاف معلومات جديدة باستعراض مجموعة من المصادر الثابتة استعراضاً متسقاً ومتواصلاً.

1- البحث

142- البحث في الإنترنت هو نشاط موجه لإنجاز مهام ويبتغى منه اكتشاف معلومات جديدة ذات صلة بهدف محدد، أو بسؤال بحثي. وينبغي أن تكون عمليات البحث متسقة ومنهجية. ويشمل ذلك استهلال البحث بسؤال واضح ومعايير بيِّنة وكلمات دالة وعوامل تشغيل[137]. وتؤدي محركات البحث وأدواته ومصطلحاته وعوامل التشغيل المختلفة إلى نتائج مختلفة. ولذلك، يجب على المحققين إبداء درجة من الإبداع والمثابرة في اتباع شتى السبل والقنوات للعثور على المعلومات المفيدة. وبالإضافة إلى محركات البحث المستخدمة للعثور على المعلومات على المواقع الشبكية المفهرسة، يمكن أيضاً استخدام البحث المنهجي على منصات التواصل الاجتماعي وداخل قواعد البيانات. ونظراً للحاجة إلى اتباع نهج متباين ومتنوع وخاص بكل حالة، ينبغي للمحققين أن يوثقوا بعناية عملياتهم بحيث يمكن شرحها في الفرع المخصص للمنهجية من التقارير، أو حين الإدلاء بشهادات بشأنها في الإجراءات القانونية. وقد تكون هذه العملية ارتجاعية فلا تسير حتماً جنباً إلى جنب مع البحث نفسه. ومع ذلك، ينبغي دائماً إجراء التوثيق في الآن نفسه قدر الإمكان. ويحبذ أن يتضمن توثيق عمليات البحث الممنهج المعلومات التالية:

(أ) الهدف وأسئلة البحث: توضيح السؤال (الأسئلة) التي يسعى البحث في الإنترنت للإجابة عنها، مع مراعاة مبدأ الموضوعية المذكور أعلاه؛

(ب) الحقائق والافتراضات والمجهولات: البدء من نقطة تكون فيها الحقائق معروفة، إن كانت هذه الحقائق قد أُثبتت. ومن المفيد أيضاً الانطلاق من المعلومات الرئيسية، أو الافتراضات المنطقية، حتى وإن لم يتم التحقق منها بعد. بيد أنَّ تسجيل أي افتراضات بصفتها تلك يُعد أمراً ضرورياً. وختاماً، قد يكون في توضيح الثغرات التي تشوب المعرفة أو غيرها من "المجهولات" في بداية التحقيق فائدة. وسيساعد تحديد هذه الفئات من المعلومات في اتقاء النتائج المنحازة أو المنحرفة بتوضيح مصطلحات البحث وبيان الأسس التي تقوم عليها؛

(ج) مصطلحات البحث والكلمات الدالة: لإجراء بحث محدد الأهداف، يجدر بالمحققين إنشاء قوائم بكلمات دالة تتسق مع مبدأ الموضوعية بناء على النظرية أو النظريات المتعددة المعتمدة في الحالة المعنية. وفي الحالة المثلى، يستخدم المحققون الكلمات الدالة في جميع اللغات والنصوص ذات الصلة ويحتاطون من أن تكون نتائج البحث مفرطة في الشمول، أو غير شاملة. وعلى الرغم من اختلاف الحالات، توجد موضوعات عامة ينبغي إدراجها في قوائم الكلمات الدالة، مثل المواقع والأسماء والمنظمات والتواريخ المهمة والوسمات (هاشتاغ) ذات الصلة. ومن المفيد أيضاً تحديد المعلومات التي يمكن أن تُعد معلومات تجريم وتبرئة في سياق تحقيق بعينه؛

(د) عمليات البحث ومحركات البحث: ينبغي على المحققين تتبع عمليات البحث التي يجرونها وتسجيل المسارات المؤدية إلى المواد المفيدة، بما في ذلك المصطلحات وعوامل التشغيل ومحركات البحث التي أفضت إلى ذلك المحتوى. ولا يلزم أن يسجل المحققون جميع نتائج البحث، لأنَّ ذلك سيكون عبئاً ثقيلاً لا حاجة إليه وذا قيمة إثباتية ضئيلة.

2- الرصد

143- ينطوي الرصد على تتبع مصدر ثابت للمعلومات، مثل موضوع بعينه مع مرور الوقت. ويكمن الهدف المنشود في تتبع المحتوى المتغير الذي ينشئه مصدر ثابت. ويتوخى في الرصد على الإنترنت أن يكون نشاطاً منهجياً يستخدم قوائم مصادر الإنترنت المعروفة والمعتمدة مسبقاً، مثل المواقع الشبكية، أو حسابات وسائط التواصل الاجتماعي، بالإضافة إلى استقصاءات البحث المجراة باستمرار لتحقيق أهداف محددة. انظر، على سبيل المثال، المصادر التالية:

(أ) المواقع الشبكية وحسابات وسائط التواصل الاجتماعي: ينبغي أن يحتفظ المحققون بقوائم عمل تبيِّن المواقع الشبكية والملامح التي يتعين رصدها وتتضمن تبريراً يبيِّن السبب الداعي إلى رصدها والشخص المسؤول عن الرصد ومن يتولى الرصد ووتيرته؛

(137) العوامل المنطقية هي كلمات بسيطة، مثل "و" و"أو" و"لا"، يمكن استخدامها "لجمع الكلمات الدالة أو استبعادها في البحث، مما يؤدي إلى نتائج أكثر تركيزاً وفائدة". انظر Alliant International University Library, "What is a Boolean operator?". يمكن الاطلاع عليه في الرابط التالي: https://library.alliant.edu/screens/boolean.pdf.

(ب) الوسمات (هاشتاغ) والكلمات الدالة: ينبغي للمحققين أيضاً الاحتفاظ بقائمة عمل تتضمن الوسمات والكلمات الدالة المرصودة؛

(ج) الأتمتة: يمكن أن تنطوي عملية الرصد على استخدام أدوات آلية تقوم، على سبيل المثال، بإجراء بحث دوري على مواقع محددة أو باستخدام بارامترات معينة. وينبغي دائماً تسجيل استخدام هذه الأدوات، بما في ذلك أسماؤها وإصداراتها والمعلومات المدخلة فيها.

3- التحيز

144- عند إجراء أنشطة بحث ورصد منهجية، يجب على الباحثين المتخصصين في المصادر المفتوحة أن يكونوا دوماً متيقظين حيال التحيز – سواء أكان ذلك تحيزهم المعرفي، أو التحيز المتأصل في المعلومات المتاحة عبر الإنترنت. فعلى سبيل المثال، إن كان المحقق يبحث عن معلومات عن الاغتصاب، فمن المرجح أن تتعلق غالبية البيانات المقدمة أو المسائل المناقشة عبر الإنترنت، باغتصاب النساء في سن الإنجاب المرتكب خارج العلاقات الزوجية. ويمكن أن تقلل نتائج البحث من الإبلاغ عن أنواع الاغتصاب الأقل وضوحاً، أو المبلغ عنها بدرجة أقل، مثل العنف الجنسي ضد الرجال والأولاد والمثليات والمثليين ومزدوجي الميل الجنسي ومغايري الهوية الجنسانية وحاملي صفات الجنسين، والنساء المسنات وحالات الاغتصاب الزوجي.

145- وثمة مثال آخر يتمثل في التحقيقات في العنف الذي يحرض عليه خطاب الكراهية المبثوث في الإنترنت، لأنَّ هذا الخطاب غالباً ما يتضمن ويعتمد على لغة مشفرة ورموز يتعذر على المحققين أو الآلات اكتشافها بسهولة. وقد لا يدرك المحققون الاستخدام الثقافي والسياقي المحدد للمصطلحات والرموز المستعملة للتحريض على الكراهية أو العنف، خاصة إن كانوا لا ينتمون إلى الجماعات المستهدفة. ومما يزيد هذا الأمر تعقيداً أنَّ خطاب الكراهية المبثوث عبر الإنترنت غالباً ما يُعد على نحو يتعذر فيه على أجهزة الرصد الآلية أو البشرية اكتشافه، وذلك تفادياً لإزالته من منصات الإنترنت، رغم أنَّه يهدف فعلاً إلى التحريض على العنف أو التمييز ضد السكان المستهدفين. وللمساعدة في تذليل صعوبة الكشف عن التحريض على التمييز، أو العداء، أو العنف، ينبغي للمحققين أن يطبقوا اختباراً قائماً على حقوق الإنسان، على النحو المنصوص عليه مثلاً في خطة عمل الرباط بشأن حظر الدعوة إلى الكراهية القومية أو العنصرية أو الدينية التي تشكل تحريضاً على التمييز أو العداوة أو العنف[138].

146- وختاماً، تتمثل أفضل طريقة يواجه بها المحققون "التحيز في الآلة" إلى جانب تحيزهم في أن يدركوا أنَّ هذا التحيز ممكن ويعترفوا بالأخطار ويتخذوا ما أمكن من خطوات فعالة لمواجهة أوجه التحيز بالبحث في المصطلحات والرموز ذات الصلة بسياق معين، أو بمجموعة من الجرائم، أو الحوادث، وبتوسيع نطاق الاستقصاء عبر الإنترنت وتنويعه. وفي حالات العنف الجنسي والجنساني، بالإضافة إلى أي جرائم أخرى يتم فيها وصم الناجين واستخدام لغة مشفرة، ينبغي على المحققين استشارة خبراء قادرين على تحديد وتبادل اللغة المشفرة وممارسات الاتصال التي غالباً ما يستخدمها هؤلاء الناجون والجناة عند التواصل في الفضاءات الإلكترونية[139].

باء- التقييم الأولي

147- قبل جمع المحتوى من الإنترنت، ينبغي للمحققين المتخصصين في المصادر المفتوحة إجراء تقييم أولي لأي مواد يحددونها، تجنباً للإفراط في جمع البيانات، وامتثالاً لمبادئ تقليل البيانات إلى أدنى حد وإجراء تحقيق مركز وحتى لا ينتهك جمع المواد حق الأفراد في الخصوصية. وحري بالمحققين المتخصصين في المصادر المفتوحة النظر في العوامل التالية ليقرروا إن كان ينبغي جمع عنصر رقمي من الإنترنت أم لا.

1- الجدوى

148- يُتوخى في التحقيقات المفتوحة المصدر أن تحدد إن كان للعنصر الرقمي المعني صلة ظاهرة بتحقيق معين. وتعتمد جدوى أي عنصر على محتواه ومصدره وعلى أهداف التحقيق والعناصر المعروفة عن الوضع. وفي مراحل التحقيق المبكرة، قد يصعب معرفة العناصر المجدية، وهو أمر قد يدفع المحققين إلى الإفراط في جمع المعلومات. بيد أنَّ المحققين المتخصصين في المصادر المفتوحة ينبغي أن يكونوا قادرين على إيضاح السبب الذي يحملهم على الاعتقاد بأنَّ العنصر المعني قد يكون مفيداً وتسجيل هذا التقييم (على سبيل المثال، باستخدام نظام بسيط وسهل الاستخدام لوضع العلامات، أو التخزين، يربط المعلومات التي تُجمع – مثلاً –

(138) انظر مفوضية الأمم المتحدة السامية لحقوق الإنسان، "حرية التعبير مقابل التحريض على الكراهية: المفوضية السامية لحقوق الإنسان وخطة عمل الرباط". يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/Ar/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx.

(139) انظر على سبيل المثال، Koenig and Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes".

بمكان، أو تاريخ، أو حادث، أو شخص، أو نوع انتهاك يجري التحقيق فيه).

2- الموثوقية

149- ينبغي للمحققين المتخصصين في المصادر المفتوحة أن يحددوا إن كانت المعلومات أو الادعاءات المذكورة في المحتوى الرقمي تبدو موثوقة للوهلة الأولى باستعراض المحتوى وتقييمه، فضلاً عن المعلومات السياقية الواردة في الملف. ويمكن أن يشمل ذلك التحقق من البيانات الوصفية المضمنة والمعلومات المرتبطة والمصدر[140]. وينبغي أن تتضمن هذه العملية محاولة لتحديد مصدر المادة الأصلي، وهو أمر يقتضي تتبع مصدر البيانات المنشورة على الإنترنت، أو الجهة التي قامت بتحميلها أو مؤلفها.

3- الإزالة

150- يجدر بالمحققين المتخصصين في المصادر المفتوحة أن يقيِّموا احتمال إزالة عنصر رقمي من الإنترنت أو من النفاذ العام إليه. وحين تكون إزالة المحتوى محتملة، يجب جمع أوثق صيغة معروفة من المحتوى حتى أثناء إجراء مزيد من التحقق والتحقيق في صيغ سابقة أو أفضل. ويمكن تقييم احتمال إزالة المحتوى باستخدام عدة عوامل من بينها هوية المصدر وموقع المحتوى وتوافق المحتوى مع شروط خدمة مقدم الخدمة. فعلى سبيل المثال، يندرج المحتوى الصادم أو المسيء الذي قد تكون له قيمة إثباتية عالية في إثبات الجرائم أو الانتهاكات في عداد أكثر المحتويات عرضة للإزالة.

4- السلامة

151- ينبغي على المحققين المتخصصين في المصادر المفتوحة أن يحددوا إن كان جمع العنصر الرقمي آمناً أو يستدعي اتخاذ احتياطات إضافية. ويرجح أن يثير جمع البيانات مخاوف إن تم من موقع شبكي قد يحتوي على عناصر تم افسادها من شأنها أن تلحق الضرر بالنظام الداخلي.

5- الواجبات اللاحقة

152- ينبغي على المحققين المتخصصين في المصادر المفتوحة تحديد الواجبات التي تنشأ عن الاحتفاظ بعنصر رقمي، مثل واجب الحفاظ عليه بطريقة آمنة للامتثال لقوانين حماية البيانات[141].

جيم- جمع البيانات

153- يتمثل جمع البيانات في فعل الحصول على معلومات منشورة على الإنترنت من خلال لقطة شاشة، أو بالتحويل إلى شكل الوثيقة المحمولة، أو تنزيل مادة تتعلق بالأدلة الجنائية، أو أي شكل آخر من أشكال الالتقاط. وبعد أن يُحدد المحتوى الرقمي وتستبين أهميته للتحقيق ويبدو موثوقاً به لأول وهلة ويُعتد به للغرض المنشود منه، ينبغي على المحقق تحديد الطريقة المناسبة لجمعه. وتختلف طرائق الجمع إن كان للمحتوى المنشور على الإنترنت قيمة إثباتية محتملة في الإجراءات القضائية، أو سيُستخدم لاتخاذ القرارات، أو سيعتمد عليه في ذلك، أو يساهم في منتج العمل الداخلي فحسب. وفي الحالات التي تتضمن منتج العمل فحسب، قد تكفي لقطة شاشة أو التحويل إلى شكل الوثيقة المحمولة. أما إن كان للمحتوى قيمة إثباتية محتملة، فقد يلزم اللجوء إلى طريقة التقاط أكثر شمولاً ونجاعة (على سبيل المثال من خلال تعيين رقم مشفَّر دال على المحتوى - انظر أدناه).

154- ويمكن جمع المحتوى المنشور على الإنترنت إما يدوياً باتباع طريقة تشغيل معيارية، أو آلياً باستخدام مجموعة متنوعة من الأدوات أو البرامج النصية. وبغض النظر عن العملية المستخدمة، يجب التقاط المعلومات المدرجة أدناه عند نقطة الجمع في أفضل الحالات. فقد تكون هذه المعلومات مفيدة لإثبات صحة عنصر رقمي. ويحتمل أن يكون لهذا الأمر أهمية خاصة في حالة الإجراءات القانونية التي يقدم فيها عنصر ما كدليل، ولا سيما في الحالات التي لا تُحدد فيها هوية المؤلف أو المنشئ، أو موقعه، أو لا يكون فيها المؤلف أو المنشئ متاحاً للإدلاء بشهادته. ويجدر بالمحققين المتخصصين في المصادر المفتوحة جمع المحتوى المنشور على الإنترنت في شكله الأصلي أو في أقرب حالة إليه، قدر المستطاع. وينبغي توثيق أي تعديلات أو تغييرات أو تحويلات تسفر عنها عملية الجمع.

155- وترد في ما يلي إرشادات بشأن ما يجب جمعه وكيفية جمعه. ويُستعان في التقاط المعلومات أدناه بأدوات عديدة متاحة أو يمكن القيام بذلك يدوياً. وبينما يُعد جمع كل المعلومات التالية من أفضل الممارسات، فإنَّ العناصر الثلاثة الأولى (المحدد المنتظم لموضع الموارد والشفرة المصدرية للغة الترميز المستخدمة في الوثائق والتقاط الصفحة الكاملة) تمثل الحد الأدنى من المعايير لتقديم الأدلة في المحاكم. وتختلف هذه المعايير قطعاً في سياقات مختلفة، وإن كان التقاط جميع العناصر المذكورة أدناه يشكل أساساً متيناً في أي سياق:

(140) انظر الفصل السادس-هاء أدناه بشأن التحقق.

(141) انظر الفصل السادس-دال أدناه بشأن الحفظ.

(أ) عنوان الشبكة المستهدفة: ينبغي تسجيل عنوان الشبكة الخاص بالمحتوى الذي يُجمع وهو يُعرف أيضاً بالمحدد المنتظم لموضع الموارد أو معرّف الموارد المنتظم؛

(ب) الشفرة المصدرية: يجب على المحققين التقاط الشفرة المصدرية للغة الترميز المستخدمة في الوثائق الخاصة بالصفحة الشبكية، إن وجدت. وتتضمن الشفرة المصدرية للغة الترميز المستخدمة في الوثائق معلومات تفوق كثيراً الجزء المرئي من الموقع الشبكي. وتساهم الشفرة المصدرية للغة الترميز المستخدمة في الوثائق في المصادقة على المواد المجمعة؛

(ج) التقاط صفحة كاملة: حري بالمحققين أولاً التقاط صورة شاشة للصفحة الشبكية المستهدفة، مع الإشارة إلى التاريخ والوقت. والسبب في هذه العملية هو الحصول على أفضل تمثيل ممكن لما شوهد وقت الجمع؛

(د) ملفات الوسائط المضمنة: في حالة تنزيل صفحة شبكية تحتوي على مقاطع فيديو أو صور، على سبيل المثال، ينبغي أيضاً استخراج هذه العناصر المحددة من الصفحة الشبكية وجمعها؛

(هـ) البيانات الوصفية المضمنة: ينبغي على المحققين جمع البيانات الوصفية الإضافية المتعلقة بالعنصر الرقمي، إن وجدت وكانت قابلة للتطبيق. وقد تختلف البيانات الوصفية تبعاً للمصادر. بيد أنَّ البيانات الوصفية الشائعة تتضمن معرِّف المستخدم الذي يقوم بالتحميل؛ ومعرِّف المنشور، أو الصورة، أو الفيديو؛ وتاريخ التحميل ووقته والعلامة الجغرافية والوسم والتعليقات والتعليقات التوضيحية؛

(و) البيانات السياقية: ينبغي أيضاً جمع المحتوى السياقي إن كانت له صلة بفهم العنصر الرقمي. ويشمل ذلك التعليقات على مقطع فيديو، أو صورة، أو منشور ومعلومات التحميل و/أو معلومات عن الجهة القائمة بالتحميل/المستخدم، مثل اسم المستخدم، أو الاسم الحقيقي، أو السيرة الذاتية. ويجدر تحديد إن كان ينبغي جمع المعلومات المحيطة بناء على خصوصيات الحالة والعنصر الرقمي؛

(ز) بيانات عملية الجمع: يجب على المحققين المتخصصين في المصادر المفتوحة تسجيل جميع البيانات ذات الصلة بعملية الجمع، مثل اسم الجهة التي تتولى مهمة الجمع وعنوان بروتوكول الإنترنت الخاص بالجهاز المستخدم لجمع المعلومات والهوية الافتراضية المستخدمة، إن وجدت، والمؤشر الزمني. وحري بالمحققين أن يتحققوا من دقة ساعة النظام. ويفضل أن يكون ذلك بمزامنتها مع خادوم بروتوكول الزمن الشبكي. ويكمن السبب من وراء هذه الخطوة في تمثيل البيانات الوصفية المتعلقة بالوقت بدقة في ما يُجمع من ملفات. وإن استُخدمت هوية افتراضية للنفاذ إلى المعلومات المجموعة، فينبغي الإشارة إلى ذلك؛

(ح) الرقم المشفَّر الدال على المحتوى: الرقم المشفَّر الدال على المحتوى هو شكل فريد من أشكال التعريف الرقمي يستعين بالتشفير ليؤكد أنَّ المحتوى المجموع فريد من نوعه ولم يُعدَّل منذ أن جُمع. وعند نقطة الجمع، يجدر بالمحققين المتخصصين في المصادر المفتوحة أن يضيفوا يدوياً رقماً مشفَّراً دالاً على المحتوى – أو تتولى أداة التجميع تلقائياً إضافة الرقم المشفَّر. وتوجد أنواع عديدة من الأرقام المشفَّرة الدالة على المحتوى يمكن الاختيار من بينها، كما أنَّ المعايير تطورت مع مرور الوقت. وينبغي للمحققين أن يقيموا نوع الرقم المشفَّر التي ينبغي استخدامه استناداً إلى المعيار المقبول حالياً[142].

156- وفي حالات الجمع الآلي، يمكن أن تتولى أدوات مصممة لجمع المحتوى والبيانات الوصفية ذات الصلة تنفيذ بعض العمليات المبيَّنة. وينبغي إعداد تقرير تقني عن كل عنصر يُجمع يتضمن المعلومات المذكورة أعلاه لإثبات صحته في وقت لاحق. وينبغي على الدوام تخزين المعلومات السياقية وجميع أنواع البيانات الوصفية والحفاظ عليها مع العنصر الرقمي، على النحو المبيَّن في الفرع التالي.

دال- الحفظ

157- يغلب عدم الاستقرار على دوام المعلومات المنشورة على الإنترنت وتوافرها؛ فمنصات التواصل الاجتماعي قد تزيل المحتوى منها وفقاً لشروط الاستخدام الخاصة بها، أو قد يرى المستخدمون إزالة المحتوى المحمَّل أو تعديله. زد على ذلك أنَّ المعلومات المنشورة على الإنترنت يمكن تجريدها بسهولة من سياقها، أو فقدانها، أو محوها، أو إتلافها[143]. وحتى تظلَّ المواد الرقمية متاحة وقابلة للاستخدام لأغراض المساءلة القانونية، فلا بد من الحفاظ عليها

(142) The United States National Institute of Standards and Technology is one organization to look to for guidance on the current standard. انظر www.nist.gov.

(143) gN, "How to preserve open source information effectively".

في الأجلين القصير والطويل[144]. ويتمثل الغرض من الحفظ الرقمي بوجه عام في إتاحة الوصول المستمر إلى المعلومات[145]. غير أنَّ الهدف المنشود من الحفظ الرقمي لأغراض المساءلة القانونية يكمن في إدارة المواد الرقمية والحفاظ عليها بطريقة تيسِّر النفاذ إليها وتضمن صحتها وتتيح استخدامها من قبل آليات المساءلة، بما في ذلك مقبوليتها في الإجراءات القانونية. وبالتالي، يتضمن الحفظ الرقمي في سياق التحقيق الحفاظ على المعلومات بمرور الوقت بحيث يظل العنصر الذي جُمع مفهوماً بشكل مستقل للمستخدمين المقصودين، مع تأكيد كافٍ على صحته.

158- ولأغراض الحفظ على المدى الطويل، ينبغي تحديث أجهزة التخزين وأشكاله حتى تظل المواد في المتناول باستخدام الأجهزة المعاصرة.

1- خصائص العنصر الرقمي الواجب حمايته والحفاظ عليه بمرور الوقت

159- وفقاً لأمناء المحفوظات، تتضمن خصائص العنصر الرقمي الواجب حمايته والحفاظ عليه بمرور الوقت صحته ومدى إتاحته وهويته واستمراره وقابليته للعرض والفهم، على النحو الموضح بإيجاز أدناه.

(أ) الصِحَّة

160- تشير الصِحَّة إلى القدرة على إثبات بقاء العنصر الرقمي دون أن يتغير عن حاله وقت جمعه. ويتطلب ذلك أن يظلَّ هذا العنصر دون تغيير أثناء وجوده في الأرشيف، أو أن تُوثَّق أي تعديلات تُدخل عليه[146].

(ب) الإتاحة

161- تشير الإتاحة إلى إتاحة العنصر الرقمي بالمعنى البسيط المتمثل في وجوده باستمرار وإمكانية استرجاعه وبالمعنى القانوني المتمثل في تأمين حقوق الملكية الفكرية المناسبة للنفاذ إلى هذا العنصر واستخدامه[147].

(ج) الهوية

162- تشير الهوية إلى القدرة على إسناد العنصر الرقمي إلى مصدره. ويجب أن يكون العنصر الرقمي قابلاً للتعريف ومميزاً عن العناصر الرقمية الأخرى، مثلاً بتسجيله باستخدام محدد للهوية، مثل رقم التعريف الفريد[148].

(د) الاستمرار

163- يشير الاستمرار إلى سلامة العنصر الرقمي وجدواه من الناحية التقنية. ويجب أن تكون تسلسلات البتات الخاصة بالعنصر الرقمي سليمة وقابلة للمعالجة والاسترجاع[149].

(هـ) قابلية العرض

164- تشير قابلية العرض إلى قدرة البشر أو الآلات على استخدام العنصر الرقمي أو التفاعل معه باستخدام الأجهزة والبرمجيات المناسبة[150].

(و) قابلية الفهم

165- تشير قابلية الفهم إلى قدرة المستخدمين المعنيين على تفسير العنصر الرقمي وفهمه[151].

2- المسائل الخاصة بالتحقيقات

166- ينبغي للمحققين أيضاً أن ينظروا في المسائل الخاصة بالتحقيق التي تنشأ أو يتوقع أن تنشأ أثناء عملية الحفظ وأن يخططوا لها.

(144) المرجع نفسه، الصفحة 143. انظر "United Nations Educational, Scientific and Cultural Organization, "Concept of digital preservation". يمكن الاطلاع عليه في الرابط التالي: https://en.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation#:~:text=Digital%20preservation%20consists%20of%20the,hardware%20tools%20acting%20on%20data.

(145) Ng, "How to preserve open source information effectively".

(146) المرجع نفسه، لاحظ أن استخدام مصطلح "الصحة" في هذا السياق يختلف عن استخدامه في سياق قانوني.

(147) المرجع نفسه.

(148) المرجع نفسه.

(149) المرجع نفسه.

(150) المرجع نفسه.

(151) المرجع نفسه.

(أ) سلسلة المسؤولية

167- تشير سلسلة المسؤولية إلى التوثيق الزمني لتسلسل الأمناء على معلومة أو دليل، وتوثيق المراقبة والتاريخ والوقت ونقل أي من هذه الأدلة وتحليله والتصرف فيه. بعد جمع العنصر الرقمي، ينبغي الحفاظ على سلسلة المسؤولية عنه بوضع نظام حفظ رقمي مناسب.

(ب) النسخة الإثباتية

168- النسخة الإثباتية هي العنصر الرقمي الذي يجمعه المحقق في شكله الأصلي ولا يجوز تحريفه أو تغييره. وينبغي تخزين العناصر الرقمية في شكلها الأصلي. ويعني ذلك الحفاظ على نسخة أصلية نظيفة من العنصر الرقمي الذي يُجمع بجميع الأشكال التي جُمع بها.

(ج) نسخ العمل

169- ينبغي إنشاء نسخة، أو نسخ، من العنصر الرقمي لأغراض التحليل وتخزينها بشكل منفصل حتى يتمكن المحققون من أداء عملهم باستخدام النسخة بدلاً من الأصل. ويتيح ذلك الحد الأدنى من التعامل مع الأصل ويقلل احتمال المساس به، أو تغييره. ويجب توثيق جميع التغييرات التي تطرأ على العنصر، بما في ذلك استنساخ نسخ منه. وينبغي استخدام نُظم تخزين منفصلة، إن أمكن ذلك، للنسخ الإثباتية ونسخ العمل.

(د) التخزين

170- يساعد التخزين على استمرار العناصر الرقمية والقدرة على العثور عليها واسترجاعها. وينبغي ألا يُنظر إلى التخزين نظرة سلبية، بل بحسبانه عملية فعالة تتضمن مهام ومسؤوليات مستمرة ومدارة، وهي تشمل التخزين الدائم الذي تضطلع فيه وسائط التخزين بدور وإدارة التسلسل الهرمي للتخزين واستبدال الوسائط وتقصي الأخطاء والتحقق من ثبات العنصر (للتأكد من عدم تغيير العنصر) واستعادة القدرة على العمل بعد الكوارث وتحديد موقع المواد المخزنة واسترجاعها[152]. ويجوز تخزين المعلومات الرقمية في الموقع (على الإنترنت أو خارجه) أو خارجه (على الإنترنت أو خارجه)[153]. وتتضمن الخيارات تخزين المحتوى الرقمي في قرص صلب محلي، أو وسيلة تخزين محلية نقالة، أو قرص شبكي يعد جزءاً من شبكة محلية، أو خادوم عن بعد، أو نظام تخزين سحابي. وتشمل الاعتبارات المتعلقة باختيار التخزين سعة التخزين (الحيز) والنفاذ والتحكم والنسخ الاحتياطية والقانون ذا الصلة وأمن المعلومات وحماية البيانات. وينبغي أيضاً أن تأخذ خيارات التخزين في الحسبان السرعة والتوافر والتكلفة والاستدامة وإدارة التخزين ونظم الاسترجاع[154].

'1' الحفظ الاحتياطي

171- في حالة فقدان البيانات أو حدوث أخطاء فيها، يمكن أن يحاول موظف المحفوظات، أو الفني، استرجاع البيانات. ومن الناحية المثالية، يتوخى أن تكون البيانات قد استُنسخت احتياطياً، أو كُررت مسبقاً في موقع منفصل. ويوصي الخبراء في تكنولوجيا المعلومات بالاحتفاظ بثلاث نسخ على الأقل من البيانات على نوعين مختلفين من أنواع التخزين على الأقل، على أن تكون نسخة واحدة على الأقل منفصلة مكانياً عن النسخ الأخرى.

'2' التردي

172- يندرج تردي الوسائط بمرور الوقت في عداد تحديات التخزين. وبوسع موظفي المحفوظات التخفيف من احتمال فشل التخزين باستخدام أنواع معمرة بشكل خاص من الوسائط. ومع ذلك، لن يسلم أي جهاز تخزين في نهاية المطاف من أن يكون به، أو يصيبه، خلل، أو يتردى، أو يتعطل بشكل عشوائي. وحتى إن لم يتعطل جهاز التخزين بشكل تام، فقد تقع أخطاء في البيانات، أو تصاب الملفات بالتلف مع تردي حالة الوسائط المخزنة. ولذلك، من المهم الاحتفاظ بنسخ احتياطية ومراقبة بنية التخزين الأساسية ودوام الملفات المخزنة بانتظام، مثل التحقق من الرقم المشفَّر الدال على المحتوى لعينات عشوائية على أساس منتظم للتحقق من عدم حدوث أي تردٍ.

'3' التقادم

173- تصبح الملفات الرقمية بالية عندما لا تكون الأجهزة اللازمة للنفاذ إلى البيانات متاحة أو لم تعد صيانتها ممكنة بشكل معقول. وكل وسيطة تخزين، بغض النظر عن متانتها، معرضة أيضاً لأن تصبح بالية على نحو يصعب، أو يستحيل، معه استرجاع البيانات المخزنة. ولذلك، ينبغي أن تحرص التحقيقات على الاحتفاظ بوسائط التخزين وتحديثها عند الضرورة، حفاظاً على إمكانية عرض البيانات وتوافرها.

(152) المرجع نفسه، الصفحة 154.

(153) Shira Scheindlin and Daniel J. Capra, *Electronic Discovery and Digital Evidence in a Nutshell* (Saint Paul, West Academic Publishing, 2009), pp. 21-22.

(154) Ng, "How to preserve open source information effectively", p. 156.

'4' *الاسترجاع*

174- قد تُحذف الملفات الرقمية خطأ أو عمداً. وعندما يقوم المستخدم "بحذف" ملف على حاسوب، يظل محتوى الملف المحذوف موجوداً على وسائط التخزين حتى يلغيه ملف آخر[155]. ولذلك، كلما زاد النشاط على حاسوب، أو وسيط تخزين آخر، ازدادت سرعة الاستبدال وأصبح الملف غير قابل للاسترجاع. وتحتوي معظم الحواسيب على أدوات مساعدة برمجية مضمنة في نظام التشغيل تتيح استرجاع الملفات المحذوفة. وبالإضافة إلى ذلك، يمكن ابتياع برمجية استرجاع البيانات واستخدامها أحياناً "لإلغاء حذف" الملفات. وقد يحتاج المحققون المتخصصون في المصادر المفتوحة إلى التماس المساعدة من متخصصين في تكنولوجيا المعلومات للنفاذ إلى البيانات المحذوفة.

'5' *التحديث*

175- يتضمن التحديث نسخ المحتوى من وسيط تخزين إلى آخر. وهو يستهدف فقط تقادم وسائط التخزين ولا يشكل استراتيجية شاملة لحفظ البيانات. ومع ذلك، ينبغي النظر إلى التحديث بصفته جزءاً لا يتجزأ من استراتيجية أوسع نطاقاً لاستبقاء البيانات[156].

هاء- التحقق

176- يشير التحقق إلى عملية إثبات دقة المعلومات التي جُمعت عبر الإنترنت، أو صحتها. ويمكن التحقق من المعلومات المفتوحة المصدر في إطار تحليل جميع المصادر - بما في ذلك المعلومات المستمدة من مصادر مغلقة وسرية - أو استناداً إلى المصادر المفتوحة حصراً. ويتألف التحقق من ثلاثة اعتبارات منفصلة هي: المصدر والعنصر أو الملف الرقمي والمحتوى ينبغي النظر إليها مجتمعة ومقارنتها نشداناً للاتساق.

1- تحليل المصادر

177- يتمثل تحليل المصادر في تقييم مصداقيتها وموثوقيتها. وتثير بيئة الإنترنت صعوبات أمام تحليل المصادر لأنَّ العديد منها يكون مجهول الهوية أو مستعار الهوية. وحتى يتسنى تحليل مصادر المعلومات بشكل سليم، يجب على المحققين المتخصصين في المصادر المفتوحة أولاً تحديد المصدر الصحيح، أو المصادر الصحيحة، لتحليله، مما يعني إسناد المعلومات إلى مصدرها الأصلي. ويشير تحليل الإسناد إلى تحديد مصدر المعلومات الرقمية وهو قد يكون موقعاً شبكياً معيناً، أو مُشتركاً، أو مُستخدماً لحساب معين، أو منصة معينة، أو هوية من ألفوا محتوى معيناً، أو أنشأوه، أو حمَّلوه. ولا يكون تحليل الإسناد ممكناً على الدوام. وهو قد يستلزم اتخاذ خطوات تحقيق إضافية على الإنترنت وفي العالم الحقيقي أو الاستعانة بتقنيات بحث وتحليل متقدمة. ومع أنَّ تحديد المؤلف مفيد، فإنَّ الافتقار إليه لا يكون، بوجه عام، أمراً حاسماً لإثبات صحة عنصر على الإنترنت؛ إذ توجد طرائق أخرى للتصديق على صحة المعلومات المفتوحة المصدر.

(أ) المصدر

178- يتعلق المصدر بأصل شيء ما، أو بأول وجود معروف له. وعندما يتعلق الأمر بالمحتوى المنشور على الإنترنت، يشير المصدر إلى أول ظهور له على الإنترنت، أو إلى العنصر الأصلي قبل تحميله على الإنترنت. وفي حالة المحتوى المنشور على الإنترنت، يفضل الإشارة إلى "النسخة الأولى التي عُثر عليها على الإنترنت" بدلاً من "النسخة الأولى على الإنترنت" لأنَّ النسخة الأصلية قد تكون أُزيلت. وحتى عندما يكون المحققون واثقين من أنهم عثروا على النسخة الأولى من شريط فيديو، أو معلومات أخرى من مصادر مفتوحة على الإنترنت، على سبيل المثال، فإنهم لا يستطيعون التأكد من مصدرها بسبب وجود قنوات مغلقة، مثل رسائل البريد الإلكتروني ومجموعات الرسائل الخاصة التي ربما استُخدمت لمشاركة العنصر قبل ظهوره علناً على الإنترنت[157].

(ب) المصداقية

179- يحتوي تاريخ نشر المصدر ونشاطه عبر الإنترنت ووجوده عليها على معلومات ذات صلة تقدح في مصداقية المصدر أو تؤيدها. ويجدر بالمحققين المتخصصين في المصادر المفتوحة النظر في وجود المصدر على الإنترنت وتاريخ نشره، وهو أمر قد يساعد في إدراك محاولة خداع متعمدة. فعلى سبيل المثال، إذا نُشر المصدر عن أحداث في بلد معين، فهل تشير المنشورات المحيطة بهذا المصدر إلى وجوده فعلاً في ذلك البلد؟

(155) Scheindlin and Capra, *Electronic Discovery and Digital Evidence in a Nutshell*, p. 24.

(156) Cornell University Library, "Digital imaging tutorial". يمكن الاطلاع عليه على الرابط التالي: http://preservationtutorial.library.cornell.edu/tutorial/preservation/preservation-03.html.

(157) على سبيل المثال، قد يرسل أحد المستخدمين صورة عبر البريد الإلكتروني إلى مستخدم آخر يقوم بعد ذلك بتحميلها على وسائل التواصل الاجتماعي. وبالتالي، تكون الصورة قد نشأت مع البريد الإلكتروني وليس المنشور.

(ج) الاستقلالية والحياد

180- ينبغي للتحقيقات أن تفحص حياد المصدر. ويمكن القيام بذلك بالنظر في أي مجموعات، أو منظمات، أو انتماءات يرتبط بها الأفراد، فضلاً عن سبل المال والجهة التي يتلقون منها التمويل. وهل هناك اتصالات أو علاقات مع أي من الأطراف المشاركة في القضية أو الحادث الذي يجري التحقيق فيه؟ وعند النظر في استقلال المصادر، ينبغي التفكير في إمكانية ربطها بالكيانات ذات الصلة (مثل أطراف النزاع). وقد تكون لأيديولوجيا المصدر، وأي انتماء لمجموعة، أهمية أيضاً. وبالنسبة لجميع المصادر، ينبغي على المحققين فحص دوافع جميع المصادر أو مصالحها أو أجنداتها الأساسية وكشفها، وإبانة مدى تأثير ذلك في صحتها.

(د) الطبيعة الخاصة

181- كلما كانت المعلومات والادعاءات دقيقة، سهُل إثباتها أو دحضها. أما التقييم النقدي للدعاوى الفضفاضة والغامضة فهو إلى الصعوبة أقرب.

(هـ) التخفيف

182- يُنظر إلى النصوص التي تُصاغ أوان الأحداث بحسبانها أوثق من نظيرتها التي تُعد بعد فترة طويلة من وقوع هذه الأحداث[158]. ويثير هذا العامل تحدياً أمام المحققين المتخصصين في المصادر المفتوحة عندما لا يكون الوقت الذي وُضع فيه النص الرقمي واضحاً.

2- التحليل التقني

183- يشير التحليل التقني إلى تحليل العنصر الرقمي نفسه، سواء أكان مستنداً، أو صورة، أو فيديو. وللتحقق من سلامة ملف، أي معرفة إن كان قد تعرض للتغيير أو المساس به أو للتعديل الرقمي، قد يستنسب المحققون المتخصصون في المصادر المفتوحة إخضاعه لفحص الأدلة الجنائية الرقمي الذي يشار إليه أحياناً باسم التحليل الاستقصائي الرقمي. وترد أدناه مكونات هذا التحليل.

(أ) البيانات الوصفية

184- البيانات الوصفية هي البيانات التي تصف بيانات أخرى وتقدم معلومات عنها. وهي قد تكون بيانات أنشأها المستخدم الذي أنشأ العنصر، أو مستخدمون آخرون، أو مزودو خدمة اتصالات، أو أي جهاز يُستخدم في إنشاء البيانات، أو نقلها، أو تلقيها، أو الاطلاع عليها. وللبيانات الوصفية دور في وصف العنصر وبيان ظروف إنشائه، أو نشره، أو تغييره. وتتضمن البيانات الوصفية مُنشِئ الملف وتاريخ إنشائه وبيانات تحميله وتعديلاته وحجمه والبيانات الجغرافية. وقد تُضمَّن البيانات الوصفية في ملف، أو تكون مرئية على صفحة شبكية، أو موجودة في الشفرة المصدرية. وقد تُنزع بعض البيانات الوصفية قبل التحميل أو أثناءه، أو نتيجة لاستخدام تطبيقات الوسائط الاجتماعية. أما إن كانت هذه البيانات متوفرة، فينبغي استعراضها عساها تساعد في إثبات الصحة. والبيانات الوصفية الأصلية عرضة للضياع لأنَّ المنصات غالباً ما تحوِّل شفرة الوسائط المحمَّلة لعرضها أو تبادلها أو ترجيعها على الإنترنت على الوجه الأمثل. وفي هذه الحالات، تكون البيانات الوصفية معبرة عن الملف الجديد لا الملف الأصلي. وعندما تُنزع البيانات الوصفية، يجدر بالباحثين في المصادر المفتوحة التماس طرق أخرى للتحقق من العنصر المعني.

(ب) بيانات شكل ملف الصور القابلة للتبديل

185- شكل ملف الصور القابلة للتبديل هو نوع من البيانات الوصفية يحدد أشكال الصور والصوت والعلامات الإضافية التي تستخدمها الكاميرات الرقمية والماسحات الضوئية والأنظمة الأخرى التي تتعامل مع ملفات الصور والصوت التي تسجلها الكاميرات الرقمية.

(ج) الشفرة المصدرية

186- الشفرة المصدرية هي البرمجة وراء أي صفحة شبكية أو برمجية. وفي حالة المواقع الشبكية، بوسع أي شخص رؤية هذه الشفرة باستخدام أدوات مختلفة، بل متصفح الشبكة نفسه. ومن السهل رؤية الشفرة المصدرية لموقع شبكي باستخدام عدد من الأدوات المتاحة مجاناً. وتتضمن هذه الشفرة محتوى وصفياً أو محتوى مخفياً أو تم المساس به وسيظهر بنية الرابط والروابط المعطلة.

3- تحليل المحتوى

187- تحليل المحتوى هو العملية التي يتم من خلالها تقييم المعلومات الواردة في فيديو، أو صورة، أو مستند، أو بيان للتأكد من صحتها وصدقها. وتحليل المحتوى متعدد الأوجه أيضاً ويتضمن تحليل القرائن المرئية أو تأكيد الصورة بالبيانات الوصفية، على سبيل المثال. وتثير خصائص بيئة الإنترنت صعوبات عديدة قد تؤثر في صحة، أو صدق، المعلومات الفعلية أو المتصورة المستمدة من المصادر المفتوحة المنشورة على الإنترنت. ويشمل ذلك الإبلاغ الدائري وإخراج المعلومات من

(158) Institute for International Criminal Investigations, *Investigators Manual*, 5th ed. (The Hague, 2012), p. 88.

سياقها وسوء تفسيرها. أما بيانات المحتوى، فهي البيانات المضمنة في العنصر الرقمي، سواء أكان فيديو، أو صورة، أو تسجيلاً صوتياً، أو مستنداً، أو نصاً غير منظم.

(أ) المُعرّفات الوحيدة

188- عند تكليف المحققين بالتحقق من محتوى مرئي، ينبغي أن يبدأوا بالبحث عن الميزات الفريدة أو التعريفية. وتشمل هذه السمات المباني والنباتات والحيوانات والأشخاص والرموز والعلامات المميزة. وينبغي توخي الحذر بشكل خاص عند تحليل السمات البشرية لتحديد هوية شخص بعينه[159]. وعادة ما تقتضي ممارسات التعريف مهارات محددة مثل المهارات المكتسبة مع مرور الوقت ومن خلال التدريب المتخصص لخبير في الأدلة الجنائية. وقد تكون التحليلات العادية غير دقيقة و/أو ضارة و/أو إشكالية بطريقة أخرى إن أجراها مهنيون غير مدربين.

(ب) معلومات يمكن التحقق منها موضوعياً

189- في كثير من الأحيان، قد يكون من المفيد البدء بتحديد ما يمكن أن يُعدَّ "معلومات يمكن التحقق منها موضوعياً". فعلى سبيل المثال، يمكن التحقق بشكل موضوعي من الطقس في يوم معين، أو من اسم قائد قوة ورتبته، أو موقع مبنى. وينبغي أن يشمل تقييم المواد المفتوحة المصدر فحصاً لمحتواها في ضوء المعلومات التي يمكن التحقق منها موضوعياً.

(ج) تحديد الموقع الجغرافي

190- تحديد الموقع الجغرافي هو تحديد، أو تقدير، موقع شيء، أو نشاط، أو الموقع الذي أُنشئ العنصر منه. فعلى سبيل المثال، قد يكون من المستطاع تحديد موقع التقاط فيديو، أو صورة فوتوغرافية تم تنزيلها من الإنترنت، باستخدام تقنيات تحديد الموقع الجغرافي. وتشمل هذه التقنيات، على سبيل المثال، تحديد المعالم الجغرافية الفريدة في صورة فوتوغرافية مع بيان موقعها الفعلي على الخريطة.

(د) التحديد الزمني

191- التحديد الزمني هو تأكيد تواريخ وأوقات الأحداث المصورة في معلومة عادة ما تكون صورة مرئية. فعلى سبيل المثال، يمكن تحديد الوقت من اليوم الذي التُقطت فيه صورة فوتوغرافية بفحص طول الظلال الناتجة عن أشعة الشمس، إلى جانب مؤشرات أخرى.

(هـ) الاكتمال

192- قد يظل المستند، أو مقطع الفيديو غير المكتمل، إثباتياً. بيد أنَّ الفجوة (الفجوات) قد تؤثر في القيمة التي تُعزى إلى العنصر المعني. ولذلك، من المهم، عند جمع معلومات مفتوحة المصدر، التقاط الملف المستهدف برمته، وعند الاقتضاء، التقاط السياق المحيط به.

(و) الاتساق الداخلي

193- يمكن إجراء تقييم للاتساق الداخلي لمعلومة واحدة مستمدة من مصدر مفتوح عبر الإنترنت، أو مجموعة من المعلومات المستمدة من مصدر بعينه (و/أو مصادر من المنشأ، أو المؤلف نفسه). ويسعى تقييم الاتساق الداخلي لمعلومة منشورة على الإنترنت إلى تحديد مدى اتساقها وتماسكها في حد ذاتها. وينبغي ألا تتناقض المعلومة، أو مجموعة من المعلومات، المتسقة داخلياً مع نفسها.

(ز) التأكيد الخارجي

194- يستمد التأكيد الخارجي من معلومات تقع خارج العنصر الرقمي نفسه ولكنها تتزامن معه وبالتالي تدعم صحة محتواه.

واو- التحليل الاستقصائي

195- التحليل الاستقصائي هو ممارسة تتمثل في استعراض المعلومات الوقائعية وتفسيرها لاستخلاص نتائج جوهرية ذات صلة باتخاذ القرارات، أو إعداد القضايا. ويتطلب حجم

(159) يتطلب تحليل الأدلة الجنائية وتحديد السمات البشرية باستخدام أدوات أو الاستعانة بالتحليل البشري (مثل التعرّف على الأشخاص من سِمات وجوههم ونظام القياس عن بعد لتحليل المشية وما إلى ذلك) خبيراً في الأدلة الجنائية. انظر Nina M. van Mastrigt and others, "Critical review of the use and scientific basis of forensic gait analysis", *Forensic Sciences Research*, vol. 3, No. 3(2018), pp. 183-193 (يمكن الاطلاع عليه في الرابط التالي: www.tandfonline.com/doi/full/10.1080/20961790.2018.1503579)؛ Royal Society and Royal Society of Edinburgh, "Forensic gait analysis: a primer for courts" (London, 2017) (يمكن الاطلاع عليه في الرابط التالي: https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf). انظر أيضاً European Network of Forensic Science Institutes, *Best Practice Manual for Facial Image Comparison* (2018) (يمكن الاطلاع عليه في الرابط التالي: http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf)؛ National Center for Audio and Video Forensics, "Height analysis of surveillance video" (يمكن الاطلاع عليه في الرابط التالي: https://ncavf.com/what-we-do/forensic-height-analysis).

المعلومات المفتوحة المصدر ونوعيتها المتفاوتة اتباع نهج جيد التنظيم في التحليل.

196- وقبل الخضوع لأنواع معينة من التحليل، قد تدعو الحاجة إلى معالجة المعلومات المفتوحة المصدر أولاً. وقد تنطوي المعالجة على ترجمة لغات أجنبية، أو تجميع مجموعات بيانات مختلفة، للمساعدة في تحليل سلوك الأفراد والمواقع والأشياء، فضلاً عن العلاقات، أو الشبكات، أو التحركات، أو الأنشطة، أو المعاملات. وتشمل المعالجة أيضاً تغيير طبيعة عنصر رقمي، أو شكله، ليتوافق مع برمجية بعينها. وتتضمن الأنواع الشائعة لمعالجة البيانات ما يلي:

(أ) الترجمة: إن كانت البيانات بلغة لا يتحدث بها المحققون أو لا تعالجها البرمجية اللازمة لاستعراض المواد، فقد يستدعي الأمر ترجمتها قبل اتخاذ مزيد من الخطوات؛

(ب) تجميع البيانات: قد يحتاج المحققون إلى تجميع مجموعات بيانات مختلفة في مجموعة بيانات واحدة أكبر من أجل تحليلها؛

(ج) إعـادة التشكيل: قد يستدعي تيسير البحث في البيانات، أو استرجاعها، أن يغيِّر المحققون تشكيل العنصر الرقمي.

197- ويستحسن معالجة نسخ العمل فقط من العنصر الرقمي، بدلاً من النسخة الأصلية أو الإثباتية. وينبغي توثيق أي معالجة للعنصر الرقمي. وإن استخدم المحققون التقنيات الرقمية لمعالجة البيانات، على سبيل المثال، فحللوا البيانات باستخدام الخوارزميات، بما في ذلك معالجة اللغات الطبيعية والتعلم العميق، فيجب أن يكونوا على دراية باحتمال التحيز في معالجة هذه البيانات.

198- وبعد معالجة المعلومات، يمكن تحليلها. وتختلف منتجات تحليل المعلومات المفتوحة المصدر حسب الغرض من معلومات المصدر الأساسية ونطاقها والجدول الزمني لإنتاجها والجمهور المعني بها. وتُعد هذه المنتجات وفقاً لاحتياجات التحقيق، وهي تشمل الرسوم البيانية والملخصات والمعاجم والقواميس والوسائل البصرية، بما في ذلك الخرائط وعمليات المسح[160].

199- وينبغي للمحققين أن يطبقوا معايير صارمة تكفل موضوعية البيانات والاستنتاجات الواردة في المنتجات التحليلية وحسن توقيتها وجدواها ودقتها وحماية الخصوصية وغيرها من اعتبارات حقوق الإنسان، لا سيما عند التعامل مع معلومات التعريف الشخصية. وينبغي ألا تُضمَّن هذه المعلومات إلا في المنتجات التي حصل المحققون بشأنها على موافقة الأشخاص المعنيين وتحقق غرضاً مباشراً في التحقيق. وينبغي أيضاً أن يُنظر إلى هذه المعلومات في ضوء القيود القانونية والأخلاقية المحيطة باستخدامها[161].

200- وتحتوي الفروع التالية على أنواع شائعة من التحليل يمكن استخدامها لتعزيز أهداف التحقيق باستخدام معلومات مفتوحة المصدر.

1- التحليل المقارن للصور/الفيديو

201- التحليل المقارن، أو علم المقارنة، هو عملية مقارنة سمات الأشياء والأشخاص و/أو المواقع بعناصر أخرى غير معروفة و/أو معروفة عندما يكون عنصر واحد على الأقل من العناصر المعنية صورة. وهو يتمثَّل في تحليل محتوى الصور ومقاطع الفيديو، بما في ذلك عناصر المقارنة بين العناصر والسمات المختلفة وجودة صورتها وإعداداتها المرئية (الضوء والمنظور وما إلى ذلك). ولئن كان العديد من الأشخاص العاديين يعرفون الآن أساسيات تحليل مقارنة الصور، فإنَّ المساعدة من خبير مؤهل ومعتمد في التحليل الجنائي للفيديو و/أو الاستدلال الجنائي الرقمي قد يساعد في توفير التحليل العلمي، بما في ذلك رأي الخبراء. وقد تستفيد أيضاً تحقيقات حقوق الإنسان وغيرها من أنواع التحقيقات من هذه الخبرة لإعطاء نتائجها وزناً أكبر.

2- التحليل التفسيري للصور/الفيديو

202- يرتبط بمقارنة الصور/الفيديو التحليل التفسيري للصورة/الفيديو الذي يتضمن تحليل عنصر رقمي لفهم محتواه المرئي. فعلى سبيل المثال، يندرج تحليل الطلقات النارية والجروح والدم والمركبات والأسلحة والأصول العسكرية، أو تحليل سرعة مركبة متحركة، أو عمر شخص في إطار التحليل التفسيري للصور/الفيديو. ويمكن أن يقوم بذلك محللون لأغراض التحقيق، أو خبراء في الأدلة الجنائية، أو خبراء في الموضوع في حالة إثبات الوقائع في الإجراءات القانونية، أو نتائج حقوق الإنسان.

3- التحليل المكاني

203- يتضمن التحليل المكاني، أو التحليل الجغرافي المكاني، تحليل المحتوى المرئي وتحليل البيانات الوصفية للعناصر التي تقدم

(160) انظر الفصل السابع أدناه بشأن الإبلاغ عن النتائج.

(161) انظر الفصل الثالث أعلاه بشأن الإطار القانوني.

إحداثيات جغرافية أو أسماء أماكن. ويتضمن التحليل المكاني فحص أجسام مختلفة وخصائص المشهد العام بدقة مناسبة والتحقق منها بمضاهاتها بصور الأقمار الصناعية، أو بغيرها من الصور والبيانات الجغرافية والخرائط ومعرفة الحالة المناسبة والسياق وأدوات نظام المعلومات الجغرافية[162].

4- حصر الجهات الفاعلة

204- حصر الجهات الفاعلة هو تقنية لفهم الجهات الفاعلة الرئيسية وتحديد علاقات القوة وقنوات النفوذ[163]. ولذلك، فهو يبدأ بتحديد الجهات الفاعلة الرئيسية ثم حصر العلاقات فيما بينها.

5- تحليل الشبكات الاجتماعية

205- على غرار حصر الجهات الفاعلة، يتمثل تحليل الشبكات الاجتماعية في رصد وقياس العلاقات بين الأشخاص والمجموعات والمنظمات والحواسيب والمحددات المنتظمة لموقع الموارد وغيرها من كيانات المعلومات/المعرفة المتصلة[164]. وغالباً ما يُشار إلى الأشخاص والمجموعات بلفظ العُقد، بينما تُظهر الروابط العلاقات بين العقد. ويستخدم تحليل الشبكات الاجتماعية الاتصالات على وسائل التواصل الاجتماعي وغيرها من الأجهزة المحمولة، أو المنصات الشبكية، لتحديد العلاقات بين الأفراد وفهمها. ويمكن أن يتولى المحقق إجراء تحليل بيانات الاتصال أو الارتباط يدوياً أو يُستعان فيه ببرمجية تحليل.

6- حصر الحوادث

206- حصر الحوادث تقنية تحليلية تُستخدم لتحديد العلاقات الزمنية والجغرافية بين حوادث مختلفة قد تشير، في سياق الانتهاكات الجنائية الدولية وانتهاكات حقوق الإنسان، إلى موقع هذه الانتهاكات أو الجرائم، بما في ذلك الأحداث السابقة واللاحقة. ويشمل ذلك أيضاً حصر الأحداث الأخرى ذات الصلة، مثل أين ومتى أدلى الجناة المدعى عليهم بأقوال.

7- تحليل نمط الجريمة/الانتهاك

207- في سياق إنفاذ القوانين الوطنية، يعني نمط الجريمة مجموعة تتألف من جريمتين أو أكثر تبلغ عنها أجهزة إنفاذ القانون أو تكتشفها وتكون جرائم فريدة من نوعها لأنها تتقاسم قاسماً مشتركاً واحداً على الأقل من قواسم نوع الجريمة وسلوك الجناة أو الضحايا وخصائص الجاني (الجناة) أو الضحايا أو المستهدفين والممتلكات المسلوبة أو مواقع حدوث هذه الجرائم[165]. وعلى المنوال نفسه، يمكن إثبات أنماط الجرائم، أو الانتهاكات، في القضايا الدولية الجنائية وقضايا حقوق الإنسان بالاستناد إلى معلومات مفتوحة المصدر.

(162) نظام المعلومات الجغرافية هو قاعدة بيانات محوسبة لإدارة البيانات المكانية وتحليلها.

(163) OHCHR, *Manual on Human Rights Monitoring*, chap. 8 on analysis, p. 24.

(164) Orgnet, "Social network analysis: an introduction". يمكن الاطلاع عليه في الرابط التالي: www.orgnet.com/sna.html.

(165) International Association of Crime Analysts, "Crime pattern definitions for tactical analysis", Standards, Methods and Technology Committee White Paper 2011-01, p. 1.

سابعاً

الإبلاغ عن النتائج

موجز الفصل

- يمكن الإبلاغ، بشكل شفهي، أو بصري، أو كتابي، عن نتائج التحقيق المفتوح المصدر الذي يشير إما إلى البيانات التي جُمعت أو إلى الاستنتاجات المستخلصة منها.
- ينبغي للمحققين أن ينظروا في أكثر الأشكال ملاءمة لولاياتهم وللجهات المستهدفة، آخذين في الحسبان عوامل مثل المعرفة التكنولوجية لدى تلك الجهات وإمكانية الوصول والموضوعية والشفافية والأمن، عند اتخاذ قرار بشأن (أ) الأشكال التي ينبغي استخدامها؛ (ب) البيانات التي ينبغي تضمينها.

208- يبيِّن هذا الفصل السبل التي يمكن اتباعها في عرض التحقيقات المفتوحة المصدر – بما في ذلك المنهجيات والبيانات الخام والنتائج التحليلية – أو الإبلاغ عنها. وفي كثير من الحالات، تُعرض المعلومات المفتوحة المصدر جنباً إلى جنب مع المعلومات الأخرى التي تُجمع باتباع أساليب التحقيق الأخرى. ويمكن أن تتخذ العروض المقدمة أشكالاً شتى، من بينها التقارير المكتوبة، أو الشفوية، أو المرئية، أو أي مزيج من هذه الأشكال. وتكون التقارير إمَّا للاستخدام الداخلي، أو للنشر الخارجي، ويمكن اعتبارها تقارير خبراء، أو غير خبراء، في ضوء عدد من العوامل. وينبغي أن تتضمن التقارير العناصر التالية:

(أ) الدقة: ينبغي أن تعرض التقارير بدقة البيانات التي جُمعت[166]. وينبغي تضمين المعلومات الإيضاحية وإيضاح أي معلومات محجوبة أو ثغرات؛

(ب) الإسناد: ينبغي أن تميز التقارير دون لبس بين المحتوى الموجود في الملك العام، أو المعلومات العامة غير السرية، والمعلومات السرية، أو المقيدة بطريقة أخرى، والمحتوى الذي يعبر عن حكم المحققين و/أو غيرهم من المهنيين أو عن رأيهم. وينبغي أيضاً للمحققين أو لغيرهم ممن يبلغون عن معلومات مفتوحة المصدر أن يتوخوا العناية الواجبة ويحصلوا على الأذونات المناسبة لاستخدام محتوى يملكه آخرون، على سبيل المثال بضمان أي حقوق ملكية فكرية ضرورية؛

(ج) الاستيفاء: ينبغي أن تتضمن النتائج مؤشراً يدل على استيفاء البيانات الأساسية، لا سيما إن استبعدت بعض البيانات عمداً؛

(د) السرية: على الرغم من وجود البيانات في سياقات مفتوحة المصدر، ينبغي أن تنظر التقارير في المواد التي يستحسن استبعادها، أو حجبها، لحماية السرية، أو لتقليل الأخطار إلى أدنى حد، ولا سيما الأخطار التي قد تتعرض لها المصادر والشهود والضحايا وأفراد المجتمعات ذات الصلة بالمعلومات المفتوحة المصدر؛

(هـ) اللغة: ينبغي أن تستخدم التقارير لغة محايدة وتتجنب اللغة الانفعالية أو العاطفية. ويُتوخى في التقارير أن تذكر الحقائق بوضوح دون الإفراط في استخدام الصفات أو وسائل التأكيد. وينبغي كتابة التقارير بلغة تراعي المنظور الجنساني. وفي أفضل الحالات، يُحبذ إتاحة التقارير العامة بلغات المجتمعات المحلية المتضررة بالإضافة إلى أي لغات رسمية يستخدمها المحققون أو هيئات التحقيق؛

(و) الشفافية: ينبغي أن تذكر التقارير بوضوح السبل التي اتبعها المحققون في أداء عملهم وتحقيق أهدافهم وعملياتهم وطرائق عملهم. وعادة ما يدرج ذلك في فرع يخص المنهجية المتبعة في التقرير، ولكن ينبغي أيضاً أن يهتدى بذلك في التوصيفات الواردة في النص برمته. وينبغي أن تكون هذه التوصيفات شفافة قدر المستطاع دون إحداث ثغرات أمنية، بالكشف عن معلومات سرية، على سبيل المثال.

ألف- التقارير المكتوبة

209- يمكن عرض التحقيق المفتوح المصدر كتابة ويجوز أن يتضمن تقارير داخلية وتقارير للعملاء، بالإضافة إلى تقارير عامة. وتتمثل إحدى طرق إبلاغ النتائج التحليلية في إعداد تقرير مكتوب يتضمن، في ما يتضمنه، تقارير من المنظمات غير الحكومية ولجان التحقيق وبعثات تقصي الحقائق والأمم المتحدة، وتقارير الخبراء المقدمة إلى محكمة أو إلى هيئة قضائية[167]. وكثيراً ما تُضمَّن المعلومات الرقمية المفتوحة المصدر مع أشكال أخرى مفتوحة ومغلقة المصدر وتحليلات. وينبغي أن تحلل التقارير المكتوبة المعلومات التي جُمعت لاستخلاص استنتاجات وتقديرات وتنبؤات منطقية منها. ويُنتظر من التقارير أن تُبيِّن اتباع منهجية سليمة وأن توضح هذه المنهجية للجمهور المستهدف. ولصحة المعلومات الأساسية الواردة في التقرير وسلامتها أهمية بالغة، فالبيانات السيئة تؤدي إلى استنتاجات رديئة[168].

210- وينبغي أن تتضمن التقارير المكتوبة الأفرع التالية، ما لم يوجد مبرر واضح لتجنب ذلك، مثل ضرورة الحفاظ على سرية بعض تقنيات التحقيق عبر الإنترنت وأساليبه ومصادره:

(أ) أهداف التحقيق: ينبغي أن تتضمن التقارير أهداف التحقيق والولايات الأساسية أو تعليمات العملاء، بما في ذلك أسئلة بحثية محددة جيداً وقابلة للصياغة؛

(166) انظر الفصل الثاني-باء أعلاه بشأن المبادئ المنهجية.

(167) للاطلاع على مثال على تقرير مكتوب عن تحقيق رقمي مفتوح المصدر، انظر، على سبيل المثال Human Rights Investigations Lab, "Chemical strikes on Al-Lataminah: March 25 & 30, 2017 - a student-led open source investigation" (Berkeley, Human Rights Center, University of California, Berkeley, School of Law, 2018).

(168) استناداً إلى الظروف ومتطلبات السرية، يوصى بإجراء استعراض من جانب النظراء لضمان دقة البيانات وجودتها، فضلاً عن التحليل والنتائج المستخلصة من تلك البيانات.

(ب) المنهجية: ينبغي أن تتضمن التقارير أساليب البحث لإتاحة التكرار وتمكين الجمهور المستهدف من فهم المعلومات ونتائج التحقيقات وتقييم مصداقيتها، بما في ذلك المجال المشمول؛

(ج) الأنشطة المنفذة: يتوخى في التقارير أن تتضمن موجزاً للأنشطة المضطلع بها وذات الأهمية للنتائج أو لتقييم جودة التحليل، بما في ذلك الأنشطة الرامية إلى تحديد البيانات الأساسية، وما تم جمعه وتحليله؛

(د) البيانات والمصادر الأساسية: ينبغي أن تتضمن التقارير سرداً للبيانات الأساسية يشمل مصادرها وجودتها؛

(هـ) الثغرات أو مواطن الارتياب: ينبغي أن تحدد التقارير أي ثغرات أو مواطن ارتياب تشوب البيانات الأساسية أو التحليل قد تكون لها أهمية جوهرية بالنسبة للنتائج؛

(و) النتائج والتوصيات: ينبغي أن تتضمن التقارير تفسيرات المحققين للبيانات أو النتائج المستندة إلى تحليلات البيانات وأن تشير إلى المحاذير والأدلة الجديدة.

باء- التقارير الشفوية

211- إن وصلت نتائج التحقيق المفتوح المصدر إلى قاعة المحكمة، فقد يكون على المحققين الإدلاء بشهاداتهم كشهود؛ ومن ثم، عرض تحقيقاتهم بالإدلاء بشهادة شفوية. ويجوز أن تشمل أشكال الإبلاغ الشفوي الأخرى تقديم عروض أمام لجان تقصي الحقائق، أو منتديات المنظمات غير الحكومية، أو المحاكم الشعبية، أو الأحداث الإعلامية.

212- ويُنتظر من أي شخص يُطلب منه تقديم نتائج تحقيقه المفتوح المصدر شفاهة أن يكون قادراً على شرح العمل شرحاً واضحاً ودقيقاً يُبيِّن المنهجية المتبعة والأدوات المستخدمة فيه حتى يتسنى معاملة الشهادة الشفوية والنتائج المبينة بما تستحقه من وزن.

213- وفي حالة الإجراءات القانونية، غالباً ما يتعين على رؤساء التحقيقات الإدلاء بشهاداتهم وينبغي أن يكونوا قادرين على التحدث عن عمل فرقهم. وهذا يتطلب، بطبيعة الحال، أن يعرفوا ما فعلته فرقهم وأن يتمكنوا من الإجابة على الأسئلة عن الأدوار المضطلع بها والمنطق الكامن وراء أي عملية اتخاذ قرار بشأن نطاق التحقيق وأساليبه والأدوات المستخدمة فيه، وما إلى ذلك. ويكون المحققون إما شهوداً خبراء أو شهوداً عاديين. ويجوز للشهود الخبراء – وهم الشهود الذين يعتبرون خبراء بسبب خبرتهم، أو معرفتهم، أو مهاراتهم، أو تدريبهم، أو تعليمهم، أو مؤهلاتهم ذات الصلة – الإدلاء بشهاداتهم عن الاستنتاجات التي توصلوا إليها وعن غيرها من نتائج العمل التحليلي. ويقتصر الشهود العاديون عموماً على الإدلاء بشهاداتهم بشأن الوقائع، وعلى وجه التحديد، الوقائع التي لاحظوها شخصياً.

جيم- التقارير المرئية

214- التمثيل البصري للبيانات هو عرض المعلومات بيانياً في شكل مخططات ورسوم بيانية وجداول وخرائط ورسوم بيانية تفاعلية تتيح طريقة سهلة لرؤية اتجاهات البيانات والقيم الناشزة فيها وأنماطها وفهمها[169]. ويمكن أن يتضمن ذلك المخططات وغيرها من العروض البيانية للبيانات مكانياً وزمانياً ورسوماً بيانية ومخططات (بما في ذلك الرسوم التي توضح الروابط الرياضية أو الاتجاهات أو العلاقات) ورسوم الشبكة البيانية التي تبيِّن العلاقات بين مختلف الأشخاص والرسوم البيانية الإحصائية. وتشكل الخرائط الثنائية والثلاثية الأبعاد للتمثيل البصري للأشياء مكانياً وزمانياً وإعادة التشكيل الثلاثية الأبعاد لمختلف المواقع، ومن بينها مسارح الجريمة، أيضاً جزءاً من عدة التمثيل البصري للبيانات[170]. وهذه الأدوات مفيدة لفهم كميات كبيرة من البيانات، وهو أمر كثير الحدوث في التحقيقات المفتوحة المصدر، أو لفهم السيناريوهات الوقائعية المعقدة فهماً أفضل.

(169) تشمل الأمثلة على التقارير المرئية في سياقات مختلفة المنصات الرقمية المستخدمة كأدلة إثباتية في قضية *المدعي العام ضد أحمد الفقي المهدي* في المحكمة الجنائية الدولية، و*المدعي العام ضد سالم جميل عياش وآخرين* في المحكمة الخاصة بلبنان؛ تقرير النتائج التفصيلية للجنة التحقيق الدولية المستقلة بشأن الاحتجاجات في الأرض الفلسطينية المحتلة (يمكن الاطلاع عليه في الرابط التالي: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf)؛ BBC Africa Eye, "Cameroon atrocity: what happened after Africa Eye found who killed this woman", BBC News, 30 May 2019 (يمكن الاطلاع عليه في الرابط التالي: www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman). انظر أيضاً generally, the work of Forensic Architecture and SITU Research.

(170) انظر على سبيل المثال، International Criminal Court Digital Platform: Timbuktu, Mali (developed by SITU Research as an asset for the *Al Mahdi* case at the International Criminal Court). يمكن الاطلاع عليه في الرابط التالي: http://icc-mali.situplatform.com. انظر أيضاً مجموعة متنوعة من التحقيقات مفتوحة المصدر عبر الإنترنت وتقاريرها المرئية في Forensic Architecture. يمكن الاطلاع عليه في الرابط التالي: https://forensic-architecture.org/methodology/osint.

215- وتتضمن الأنواع الأخرى من التمثيل البصري للبيانات ما يلي:

(أ) الخرائط الذهنية: الخريطة الذهنية هي وسيلة رسومية بيانية لتمثيل الأفكار والمفاهيم وكيفية ارتباطها بعضها ببعض. وتقوم الخرائط الذهنية بهيكلة المعلومات بطريقة تُيسِّر تحليلها وتوليفها وفهمها. وغالباً ما تتضمن الخرائط الذهنية شرحاً لكيفية اكتشاف البيانات الأساسية؛

(ب) الرسوم التخطيطية: الرسم التخطيطي هو تمثيل رسومي لسلسلة من الأحداث، مثل الخطوات المضمنة في خوارزمية، أو سير العمل، أو عمليات مماثلة؛

(ج) الرسوم البيانية التفاعلية: الرسم البياني التفاعلي هو تمثيل بياني لفكرة أو مفهوم. ويمكن استخدامه لتمثيل المعلومات الإحصائية.

216- ويجوز عرض المعلومات المفتوحة المصدر بطرق شتى تتراوح بين العرض السمعي البصري لشريط فيديو واحد، أو موقع شبكي واحد، وبين العروض التفاعلية والرقمية والمجمعة المتعددة الوسائط[171]. ويمكن استخدام العروض التوضيحية والرسوم التوضيحية المرئية، أو المنصات الرقمية، لعرض المعلومات بطريقة تسهل على الجهات المستهدفة فهم الحقائق الأساسية. ومن الأمثلة على ذلك الجداول الزمنية والصور المركبة (مثل عرض مسرح الجريمة بزاوية 360 درجة) ومقاطع الفيديو المعدلة.

217- وفي حالة تقديم تمثيل بصري للبيانات وأدلة متعددة الوسائط في قاعة المحكمة، أو إلى جهات متلقية عامة أخرى، ينبغي للمحققين أن يفهموا المسائل التقنية التي قد تنشأ، بما في ذلك المنصات التي قد يحتاج إليها المحامون لتقديم عروضهم التقديمية بشكل مفيد قدر الإمكان لمن يتقصون الحقائق. وينبغي أن تؤخذ مجموعة من العوامل في الحسبان عند تحديد أفضل شكل لتمثيل البيانات الأساسية. وتشمل هذه العوامل الجهات المتلقية المستهدفة ومدى ألفتها مع الأشكال المحتملة وقدرتها على فهم المعلومات المقدمة. وفي نهاية المطاف[172]، ينبغي أن تعزز جميع العروض هدف إلقاء الضوء على الوقائع ذات الصلة بقضية ما بطريقة إثباتية وغير ضارة وأن تمتثل للمتطلبات القانونية والأخلاقية للولاية القضائية التي تُقدم فيها المعلومات.

(171) أنتج فريق التحقيقات البصرية في صحيفة نيويورك تايمز عدداً من التفسيرات المرئية المصممة لتجميع المعلومات المفتوحة المصدر على الإنترنت ودعم تحليل الحوادث المعقدة والإبلاغ عن تلك النتائج، ولكن هذه التفسيرات لم تُقدم إلى محكمة. انظر، على سبيل المثال، Nicholas Casey, Christoph Koettl and Deborah Acosta, "Footage contradicts U.S. claim that Nicolás Maduro burned aid convoy", *New York Times*, 10 March 2019 (يمكن الاطلاع عليه في الرابط التالي: www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html). Malachy Browne and others, "10 minutes. 12 gunfire bursts. 30 videos. Mapping the Las Vegas massacre", *New York Times*, 21 October 2017 (يمكن الاطلاع عليه في الرابط التالي: www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

(172) انظر Alexa Koenig, "Open source evidence and human rights cases: a modern social history", in *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig and Daragh Murray, eds. (Oxford, Oxford University Press, 2020), pp. 38-40.

ثامناً

مسرد المصطلحات

موجز

- المصطلحات والتعاريف المستخدمة في التحقيقات المفتوحة المصدر أو تلك التي قد ترد في موارد مفيدة أو ذات صلة.

218- يحتوي هذا الفصل على مصطلحات وتعاريف يُعتقد أنَّها ذات فائدة للمحققين المتخصصين في المصادر المفتوحة. ولا تُستخدم جميع المصطلحات في هـذا البروتوكول ولكنها أُدرجت في هذا المسرد لأنها قد ترد في موارد مفيدة أو ذات صلة.

ثغرة هوائية: عندما لا يكون الجهاز الرقمي متصلاً اتصالاً مباشراً بالإنترنت أو أي شبكة، متيحاً بذلك الأمان للمعلومات التي يحتفظ بها هذا الجهاز.

الخوارزمية: إجراء محدد تحديداً جيداً، أو مجموعة من التعليمات، تتيح للحاسوب حل مشكلة، أو الاستجابة لسيناريو محدد سلفاً.

إغفال الهوية: عملية يستحيل معها تحديد هوية فرد بعينه.

واجهة برمجة التطبيقات: شفرة تتيح لبرامج برمجيات الحاسوب التواصل بعضها مع بعض.

الذكاء الاصطناعي: فرع من علوم الحاسوب مخصص لإعداد برمجة للآلات لتتعلم كيف تتفاعل مع متغيرات غير معروفة وتتكيف مع بيئات جديدة.

المُرشد: آلية لتتبع نشاط المستخدم وسلوكه. وتتكوّن المُرشدات من عنصر صغير لا يكون اقتحامياً (غالباً ما يكون غير مرئي) في صفحة شبكية (وتكون بدرجة صغر بيكسل واحد شفاف) ينقل، عندما يدفع به المتصفح، تفاصيل عن المتصفح والحاسوب اللذين يستخدمهما طرف ثالث.

البيانات الضخمة: مجموعات البيانات الكبيرة التي يمكن تحليلها للكشف عن الارتباطات بين نقاط البيانات وإبراز الأنماط التي قد تساعد في القدرات على التنبؤ. وتتمثل الخصائص الرئيسية للبيانات الضخمة في الحجم والتعقيد.

تقنية سلسلة الكتل: تقنية قائمة على التشفير تتيح استخدام سجل مفتوح وموزع يتكون من "كتل" لتسجيل معاملات بين طرفين أو كيانين بكفاءة وبطريقة دائمة يمكن التحقق منها.

البحث المنطقي: تقنية للبحث على الإنترنت تتيح للمستخدمين جمع الكلمات الدالة مع عوامل التشغيل أو المعدلات (أي و، لا، أو) لتضييق نطاق نتائج البحث ومن ثم إتاحة نتائج بحث أكثر ملاءمة وتحديداً.

حروف التحقق (Captcha): اختصار لاختبار تورينج العام المؤتمت بالكامل للتمييز بين الحواسيب والبشر وهو نوع من اختبار التحدي والاستجابة المستخدم في الحوسبة لتحديد إن كان المستخدم إنساناً أم لا.

غرفة التحادث الإلكترونية: موقع شبكي على الإنترنت يتيح للمستخدمين إجراء محادثات في الوقت الفعلي عبر الإنترنت.

الحوسبة السحابية: نموذج عمليات يتيح تخزين البيانات ومعالجتها وتحليلها عبر شبكة داخلية، أو عبر الإنترنت. وهناك ثلاثة أنواع سحابية: خاصة وعامة وهجينة.

ملف تعريف الارتباط: جزء صغير من البيانات يرسله موقع شبكي ويُخزَّن إما في ذاكرة الحاسوب الخاصة بالمستخدم أو يُكتب على قرص الحاسوب ليستخدمه المتصفح. وغالباً ما تكون ملفات تعريف الارتباط ضرورية ليعمل الموقع الشبكي بكفاءة – وهي تتيح القدرة على تخزين أفضليات الموقع الشبكي الخاص بالمستخدم وتفاصيل هويته، مزيلة الحاجة إلى إدخال البيانات باستمرار من قبل المستخدمين أثناء زياراتهم اللاحقة.

التوقيع المشفَّر: عملية رياضية للتحقق من صحة عنصر رقمي. وباستخدام خوارزمية، يمكن للمرء إنشاء مفتاحين مرتبطين رياضياً: أحدهما خاص والآخر عام. ولإنشاء توقيع رقمي، تُستخدم برمجية لإنشاء رقم مشفَّر للبيانات الإلكترونية. ويُستخدم المفتاح الخاص لتشفير الرقم.

التشفير: ممارسة تشفير المعلومات، أو فك تشفيرها رقمياً.

الشبكة الخفية: ذلك الجزء من الإنترنت الذي لا يمكن النفاذ إليه إلا باستخدام برمجية خاصة، مما يتيح للمستخدمين ومشغلي المواقع الشبكية البقاء مجهولي الهوية ويحول دون تعقبهم.

التنقيب في البيانات: ممارسة فحص واستخراج البيانات من قواعد البيانات لاستنباط معرفة، أو معلومات جديدة.

الأرشيف الرقمي: مجموعة من الوثائق، أو الصفحات الشبكية، أو السجلات الإلكترونية. ويشير هذا المصطلح أيضاً إلى منظمة رسمية، أو غير رسمية، تقبل مسؤولية الحفاظ على المعلومات وإتاحتها للمستخدمين المأذون لهم بذلك.

الحفظ الرقمي: السياسات والاستراتيجيات اللازمة لإدارة المعلومات الرقمية والحفاظ عليها بقيمة دائمة مع مرور الوقت، بحيث تكون المعلومات الرقمية متاحة وقابلة للاستخدام من قبل المستخدمين المستهدفين في المستقبل.

اسم النطاق: تسمية تحدد نطاق الشبكة. وفي إطار الإنترنت، يتم تشكيل أسماء النطاقات وفقاً لقواعد وإجراءات نظام أسماء النطاقات.

وبوجه عام، يمثل اسم النطاق مورداً لبروتوكول الإنترنت، مثل حاسوب شخصي يُستخدم للنفاذ إلى الإنترنت، أو خادوم يستضيف موقعاً شبكياً، أو الموقع الشبكي نفسه، أو أي خدمة أخرى يتم إيصالها عبر الإنترنت.

مسجل اسم النطاق: الشخص، أو الشركة، أو الكيان الآخر الذي يمتلك اسم نطاق أو يحوزه.

نظام أسماء النطاقات: النظام الذي يُستخدم لتنظيم عملية تخصيص أسماء النطاقات.

شبكة الجمع والمراقبة (Dragnet): في سياق الإنترنت، نظام جمع، أو مراقبة، آلي واسع النطاق.

البيانات المضمنة: البيانات المخزنة في ملف مصدر، أو صفحة شبكية.

التشفير: عملية تتمثل في جعل البيانات غير قابلة للنفاذ إليها دون مفتاح فك التشفير.

الرقم المشفَّر أو الرقم المشفَّر الدال على المحتوى: الحسابات التي يمكن تطبيقها على أي نوع من الملفات الرقمية لإنشاء سلسلة أبجدية رقمية ثابتة الطول يمكن استخدامها كدليل على عدم تعديل ملف رقمي. وتبقى هذه السلسلة كما هي في كل مرة يتم فيها تطبيق الحساب طالما لم يتغير الملف.

لغة الترميز المستخدمة في الوثائق: لغة برمجة تُستخدم لتصميم الصفحات الشبكية التي يتم النفاذ إليها باستخدام متصفح الشبكة.

بروتوكول نقل النص المترابط: بروتوكول أساسي للإنترنت يحدد كيفية نقل البيانات وتلقيها.

هيئة الإنترنت للأرقام المخصصة: منظمة تشرف على التخصيص العالمي لعناوين بروتوكول الإنترنت وأرقام الأنظمة المستقلة وأنظمة أسماء النطاقات.

هيئة الإنترنت للأسماء والأرقام المخصصة: منظمة مسؤولة عن ضمان التشغيل المستقر والآمن للإنترنت بتنسيق صيانة وإجراءات العديد من قواعد البيانات المتعلقة باسم الإنترنت وفضاءاته الرقمية.

منتدى الإنترنت (المعروف أيضاً باسم المنتدى الإلكتروني): موقع شبكي يتيح للمستخدمين نشر الرسائل والتحادث. وتحتوي المنتديات عادة على رسائل أطول من تلك التي تظهر في غرف التحادث الإلكترونية ويُرجح بدرجة أكبر أن تقوم بأرشفة المحتوى.

عنوان بروتوكول الإنترنت: لكل جهاز رقمي يتصل بالإنترنت عنوان بروتوكول الإنترنت. ويوجد نوعان من عناوين بروتوكول الإنترنت هما بروتوكول الإنترنت – الإصدار 4 (رقم 32 بت) وبروتوكول الإنترنت – الإصدار 6 (رقم 128 بت). ويُستخدم عنوان بروتوكول الإنترنت لتحديد الحواسيب والأجهزة الأخرى على الإنترنت.

مقدم خدمات الإنترنت: كيان يقدم لمستخدمي الإنترنت خدمات للنفاذ إلى الإنترنت واستخدامه.

الشبكة الداخلية (الإنترانت): شبكة حاسوبية خاصة تستخدم بروتوكولات الإنترنت والاتصال بالشبكة لإنشاء نسخة داخلية من الإنترنت.

الشبكة المحلية: مجموعة من الأجهزة الرقمية متصلة بالشبكة نفسها في موقع فعلي محدد.

التعلم الآلي: نوع من الذكاء الاصطناعي يستخدم تقنيات إحصائية لإعطاء الحواسيب القدرة على "التعلم" من البيانات، دون أن يتم برمجتها صراحة.

البرمجيات الخبيثة: البرمجيات الخبيثة المصممة لإلحاق الضرر بجهاز رقمي، أو بشبكة، أو بخادوم، أو بمستخدم. وتوجد أنواع عديدة مختلفة من البرمجيات الخبيثة من بينها الفيروسات وأحصنة طـروادة وبرمجيات انتزاع الفدية وبرمجيات الدعاية وبرمجيات التجسس الحاسوبي.

البيانات الوصفية: هي بيانات عن البيانات. وهي تحتوي على معلومات عن ملف إلكتروني مضمَّن في الملف أو مقترن به. وغالباً ما تتضمن البيانات الوصفية خصائص الملف وتاريخه، مثل اسمه وحجمه وتواريخ إنشائه وتعديله. وقد تبيِّن البيانات الوصفية كيف ومتى ومن جمع الملف الرقمي وأنشأه ونفذ إليه وعدَّله وشكَّله.

الملف الأصلي: هو ملف بتشكيله الأصلي.

صيغة الوثيقة المحمولة (PDF): صيغة ملف ثابت يحافظ على شكل الوثيقة (بما في ذلك البُنط والمسافات والصور) بغض النظر عن البرامج والأجهزة وأنظمة التشغيل المستخدمة لفتح تلك الوثيقة ومشاهدتها. ويؤدي تحويل ملف من صيغته الأصلية إلى صيغة الوثيقة المحمولة إلى انتزاع بياناته الوصفية، مما يتيح صورة ثابتة للوثيقة.

برنامج التنبؤ: برنامج يستخدم الخوارزميات التنبؤية والتعلم الآلي لتحليل البيانات لإجـراء تنبؤات بشأن الأحـداث، أو السلوكيات المستقبلية، أو غير المعروفة.

إخفاء الهوية: معالجة البيانات الشخصية بطريقة لا يمكن بعدها أن تُنسب المعلومات إلى موضوع بيانات معين دون استخدام معلومات إضافية.

استخراج البيانات: طريقة لاستخراج كميات كبيرة من البيانات من المواقع الشبكية.

الهندسة الاجتماعية: التلاعب النفسي بشخص للتمكن من النفاذ غير المأذون به إلى المعلومات، وهو شبيه بالقرصنة ولكنه ينطوي على استغلال ثغرة بشرية بدلاً من ثغرة تقنية. وتوجد أنواع مختلفة عديدة من الهندسة الاجتماعية، من بينها استراق الهوية الرقمية والتصيد الاحتيالي الموجه.

الانتزاع: عملية تكنولوجية لإزالة البيانات الوصفية من ملف دون تحويل هذا الملف إلى تشكيلات أخرى.

البيانات المنظمة: البيانات، أو المعلومات، التي تتوافق مع تشكيل جامد في مستودع (عادة ما تكون قاعدة بيانات ولكن يمكن أن تكون أيضاً مجموعة من النماذج المملوءة) بحيث تكون عناصرها متاحة بسهولة للمعالجة والتحليل.

الشبكة السطحية: ذلك الجزء من الإنترنت الذي يمكن النفاذ إليه باستخدام أي متصفح والبحث فيه باستخدام محركات البحث التقليدية.

المتتبع: نوع من ملفات تعريف الارتباط يستغل قدرة المتصفح على الاحتفاظ بسجل للصفحات الشبكية التي تمت زيارتها ومعايير البحث التي تم إدخالها وما إلى ذلك. وأجهزة التتبع هي عموماً ملفات تعريف ارتباط دائمة تحتفظ بسجل قيد التشغيل لسلوك زائر معين.

بيانات الحركة: أي بيانات تتم معالجتها لغرض نقل المعلومات على شبكة اتصالات إلكترونية أو للفوترة المتعلقة بذلك الاتصال. وتشمل هذه البيانات البيانات المتعلقة بتوجيه الاتصال، أو وقته، أو مدته.

المحدد المنتظم لموقع الموارد: موقع الصفحة الشبكية على الإنترنت. وهو مثله مثل العنوان الشبكي نفسه.

البيانات غير المنظمة: البيانات والمعلومات التي تأتي في أشكال مختلفة عديدة ولا يتم تنظيمها في شكل جامد ومن ثم لا تسهل معالجتها وتحليلها. وعادة ما تكون نصاً، ولكنها يمكن أن تتضمن أيضاً ملفات الصور والصوت والفيديو.

الآلة الافتراضية: برنامج يحاكي نظام الحاسوب.

الشبكة الخصوصية الافتراضية: شبكة آمنة أو نظام من العقد الآمنة التي تستخدم التشفير وعمليات الأمان الأخرى حتى يقتصر النفاذ إلى الشبكة على المستخدمين المأذون لهم فقط. وتخفي الشبكات الخصوصية الافتراضية عنوان بروتوكول الإنترنت وتمنع اعتراض البيانات.

مزود الخدمة على شبكة الإنترنت: كيان يقدم خدمات ومنتجات على الإنترنت، مثل شركة وسائل التواصل الاجتماعي.

المفهرس الآلي (يشار إليه أيضاً باسم عنكبوت الشبكة، أو العنكبوت الزاحف): برنامج يتصفح الإنترنت بشكل منهجي وفقاً لنص آلي لتنزيل المواقع الشبكية التي تمت زيارتها وفهرستها.

بروتوكول الإجابة على الاستفسارات: سجلّ يحدد من يملك اسم نطاق معين استناداً إلى الكيان الذي سجله. وقد يستخدم المحققون المتخصصون في المصادر المفتوحة بروتوكول الإجابة على الاستفسارات كجزء من عملية تحليل المصدر والتحقق منه.

الشبكة العالمية: فضاء معلومات تُحدد فيه الوثائق وغيرها من الموارد الشبكية بواسطة المحددات المنتظمة لمواقع الموارد والتي قد تكون مترابطة بواسطة وصلة ربط نصي إلكتروني ويمكن النفاذ إليها من خلال الإنترنت. ويمكن للمستخدمين النفاذ إلى موارد الشبكة العالمية باستخدام تطبيق برمجي يسمى متصفح الشبكة.

المرفقات

موجز

- نموذج خطة التحقيق عبر الإنترنت
- نموذج تقييم التهديدات والأخطار الرقمية
- نموذج تقييم المشهد الرقمي
- استمارة جمع البيانات عبر الإنترنت
- اعتبارات للتحقق من صحة الأدوات الجديدة

المرفق الأول

نموذج خطة التحقيق عبر الإنترنت

رقم التحقيق المرجعي:	
تاريخ التقييم:	
موجز التحقيق: *موضوع التحقيق ونطاقه المكاني والزماني*	

1- الأهداف والأنشطة المقررة

يشمل ذلك أهداف التحقيق عبر الإنترنت واستراتيجيته، فضلاً عن أنشطة محددة مشفوعة بجدول زمني لتنفيذها.

2- ملخص تقييم المشهد الرقمي

يشمل ذلك تقييماً للمشهد الرقمي في المنطقة الجغرافية الخاضعة للتحقيق، مثل وسائل التواصل الاجتماعي الشائعة والتطبيقات النقالة وغيرها من التقانات، فضلاً عمن يمكنه النفاذ إلى هذه التقانات واستخدامها.

3- استراتيجية التخفيف من الأخطار وتدابير الحماية

يشمل ذلك النتائج الرئيسية لتقييم التهديدات والأخطار الرقمية، إلى جانب استراتيجية لتحديد هذه التهديدات وإدارتها والتصدي لها.

4- حصر الجهات الفاعلة ذات الصلة

يشمل ذلك قائمة بالمستجيبين الأوائل الذين ربما جمعوا محتوى منشوراً على الإنترنت يحتمل أن يكون ذا صلة واختفى منذ ذلك الحين ومحفوظات رقمية ومقدمي خدمات الإنترنت والخدمات الشبكية الذين قد تكون بحوزتهم إصدارات أصلية أو بيانات وصفية إضافية للمحتوى المنشور على الإنترنت يمكن الحصول عليها بتقديم طلب لالتماس المساعدة. ومع أنَّ المحققين غير القانونيين قد لا يتمتعون بالسلطة القانونية لطلب معلومات مغلقة المصدر، فإنَّ الاتصالات بين مقدمي خدمات الإنترنت قد تكون ذات قيمة في الإجابة على الأسئلة ومساعدة المستخدمين في التنقل في منصاتهم.

5- الأدوار والمسؤوليات

يشمل ذلك تحديد أدوار أعضاء الفريق ومسؤولياته. وينبغي أن يشمل ذلك تحديد جهة تنسيق تتولى تنسيق الأنشطة عبر الإنترنت. ويمكن أن يشمل ذلك أيضاً تقييماً لمن يحتمل أن يكون مسؤولاً إن دُعي للإدلاء بشهادته في المحكمة.

6- الموارد

يشمل ذلك تقييماً للاحتياجات من الموظفين (أعداد المحققين وتنوع الموظفين وشمولهم)، فضلاً عن أي تدريب متخصص ومعدات لازمة لأنشطة التحقيق عبر الإنترنت.

7- التوثيق

يشمل ذلك توجيهات محددة حول كيفية ومكان قيام أعضاء الفريق بتوثيق أنشطتهم الاستقصائية عبر الإنترنت.

المرفق الثاني

نموذج تقييم التهديدات والأخطار الرقمية

رقم التحقيق المرجعي:	
تاريخ التقييم:	
موجز التحقيق: *موضوع التحقيق ونطاقه المكاني والزماني*	
أهداف التحقيق:	

1- ما هي الأصول (الموجودات) المتوفرة لديك؟

الأشخاص (مصنفون جنسانياً):	
الأصول المادية:	
الأصول غير المادية (مثل البيانات):	

2- ما هي مواطن الضعف لديك؟

3- ما هي أنواع التهديدات التي يمكن أن تستغل مواطن الضعف هذه وتضر بأصولك؟

4- ما هي الجهات الفاعلة المُهدِّدة المحتملة؟

ألف - ما هي مصالحها؟	
باء - ما هي قدراتها؟	
جيم - ما هو احتمال وقوع هجوم؟	

5- ما هي تدابير التخفيف من الأخطار الممكنة/المناسبة؟ هل ثمة حاجة للتصدي للأخطار المختلفة التي تواجهها الأجناس المختلفة؟

ينبغي مراعاة ما يلي:

- الضرر المادي
- الضرر الرقمي
- الضرر النفسي

المرفق الثالث

نموذج تقييم المشهد الرقمي

رقم التحقيق المرجعي:	
تاريخ التقييم:	
موجز التحقيق: *موضوع التحقيق ونطاقه المكاني والزماني*	
أهداف التحقيق:	

تشير العلامة النجمية (*) إلى أنَّ المحققين ينبغي أن يراعوا عوامل مختلفة مثل العمر ونوع الجنس والموقع وغيرها من المعلومات الديموغرافية ذات الصلة.

1-	الأطراف ذات الصلة (أي مجتمعات محلية محددة، وجماعات مسلحة، وما إلى ذلك). يُرجى تحديد ما إذا كان هناك أي اختلاف في استخدام التكنولوجيا أو التمثيل عبر الإنترنت حسب نوع الجنس أو العمر أو الإعاقة بين كل من الأطراف.
2-	اللغات ذات الصلة (بما في ذلك اللغة العامية ولغات المطلعين على بواطن الأمور الأخرى)*
3-	محركات البحث المستخدمة بشكل متكرر*
4-	منصات التواصل الاجتماعي المشهورة*
5-	المواقع الشبكية المشهورة*
6-	استخدام/انتشار الإنترنت (مصنف جنسانياً وعمرياً، وما إلى ذلك)
7-	أفضليات الهاتف المحمول/نظام التشغيل (مصنفة جنسانياً وعمرياً، وما إلى ذلك)
8-	تطبيقات الهاتف المحمول الشائعة (مصنفة جنسانياً وعمرياً، وما إلى ذلك)
9-	مقدمو خدمات الاتصالات السلكية واللاسلكية
10-	الاتصال: مواقع أبراج تقنية الاتصال اللاسلكي – Wi-Fi/الخلوية
11-	القوانين ذات الصلة (حرية التعبير، الوصول إلى المعلومات، الخصوصية)
12-	وسائل الإعلام والمراسلين (الوجود على الإنترنت)
13-	قواعد البيانات المفتوحة (مثل البيانات الحكومية وبيانات المنظمات غير الحكومية/الباحثين)
14-	قواعد البيانات المدفوعة الأجر (مثل البيانات الحكومية وبيانات الشركات الخاصة/الباحثين)
15-	مدى تمثيلية المحتوى المنشور على الإنترنت (بما في ذلك المجموعات المستبعدة)

المرفق الرابع

استمارة جمع البيانات عبر الإنترنت

1- جامع المعلومات

التحقيق:

جامع البيانات:

عنوان بروتوكول الإنترنت الخاص بجامع البيانات:

بدء جمع البيانات (التاريخ/المؤشر الزمني):

نهاية جمع البيانات (التاريخ/المؤشر الزمني):

2- المعلومات المستهدفة

العنوان الشبكي (المحدد المنتظم لموقع الموارد):

الشفرة المصدرية للغة الترميز المستخدمة في الوثائق:

لقطة الشاشة:

البيانات المُجمَّعة:

عنوان (عناوين) بروتوكول الإنترنت:

3- معلومات حزمة جمع البيانات

اسم ملف حزمة جمع البيانات:

قائمة الرقم المشفَّر الخاص بحزمة التجميع:

الرقم المشفَّر الدال على المحتوى الخاص بحزمة جمع البيانات:

4- الخدمات المستخدمة

منتج (منتجات) البرمجيات:

الخدمة الزمنية:

خدمة بروتوكول الإنترنت:

خدمة بروتوكول الإجابة على الاستفسارات:

المرفق الخامس

اعتبارات التحقق من صحة الأدوات الجديدة

السمات
الشفرة المفتوحة المصدر مقابل الشفرة المغلقة المصدر
المدفوع الأجر مقابل المجاني
هوية المالك (فرد أو شركة) أو انتماءاته أو اهتماماته
التمويل (كيف تُمول الأداة وإلى أي مدى؟ ما هو عمر المنتج المحتمل؟)
الأسئلة الأمنية
من يملك الأداة أو الشفرة الأساسية؟
هل الشفرة الأساسية مفتوحة المصدر أم مغلقة المصدر؟
هل يتم التحقق من الأداة بشكل مستقل؟
أين ستُخزَّن أي بيانات تُجمع؟
من يُتاح له النفاذ إلى أي بيانات تُجمع؟
ما هي بنية الأمن الأساسية الخاصة بالأدلة؟
ما هي الالتزامات القانونية التي قد تؤثر في أمن استخدام الأداة؟
إن حدث انتهاك للقانون، هل يوجد حق في الانتصاف؟
الاسئلة الوظيفية
ما هي وظيفة الأداة؟
ما هي قابلية الأداة للاستخدام؟
ما هي قدرة المالك، أو المزود، أو مستخدم الأداة على تقديم الدعم؟
ما هي وتيرة تحديث الأداة؟
ما مدى توافق الأداة مع الأنظمة الأخرى؟

مكتب مفوضية الأمم المتحدة السامية لحقوق الإنسان
Palais des Nations
CH 1211 Geneva 10, Switzerland
Email: ohchr-infodesk@un.org
Website: www.ohchr.org/ar

HUMAN RIGHTS CENTER
UC Berkeley School of Law

University of California
Human Rights Center (HRC)
2224 Piedmont Avenue
Berkeley, CA 94720
Email: hrc@berkeley.edu
Website: https://humanrights.berkeley.edu/

ISBN: 978-92-1-154247-9

Co-published by the United Nations, on behalf of the Office of the United Nations High Commissioner for Human Rights, and the Human Rights Center at the University of California, Berkeley, School of Law.

Printed at United Nations, Geneva – 2012695 **(A)** – January 2024 – 1,384 – **HR/PUB/20/2**