مجلة
البوصلة الرقمية

المجلة الليبية لقانون الانترنت

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

العدد الثاني
سبتمبر
2025

The Digital Compass

Libyan Journal of CyberLaw

Issue No. 2 – September 2025

إدارة مكافحة جرائم تقنية المعلومات

مجلة
البوصلة الرقمية

المجلة الليبية لقانون الانترنت

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

العدد الثاني
سبتمبر 2025

مجلة البوصلة الرقمية
المجلة الليبية لقانون الانترنت

السنة الأولى
العدد الثاني
2025

صَدَرَت هذه المجلة بموجب:

قرار رئيس جهاز المباحث الجنائية رقم (214) لسنة 2025م
بشأن إنشاء مجلة علمية دورية متخصصة.

قرار مدير إدارة المطبوعات والمصنفات الفنية رقم (07) لسنة 2025م
بشأن الإذن بإصدار مجلة علمية إلكترونية.

رقم الايداع القانوني / 294 - 2025 دار الكتب الوطنية

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

تمت طباعة هذا العدد بدعم من شركة آفاق الود للتدريب والاستشارات

مجلة البوصلة الرقمية

مجلة رقمية علمية –قانونية- توعوية – دورية، تصدر بصفة فصلية عن إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية، وتُعنى بتسليط الضوء على قضايا العالم الافتراضي بمختلف أبعاده.

تتناول المجلة موضوعات شاملة في مجال:

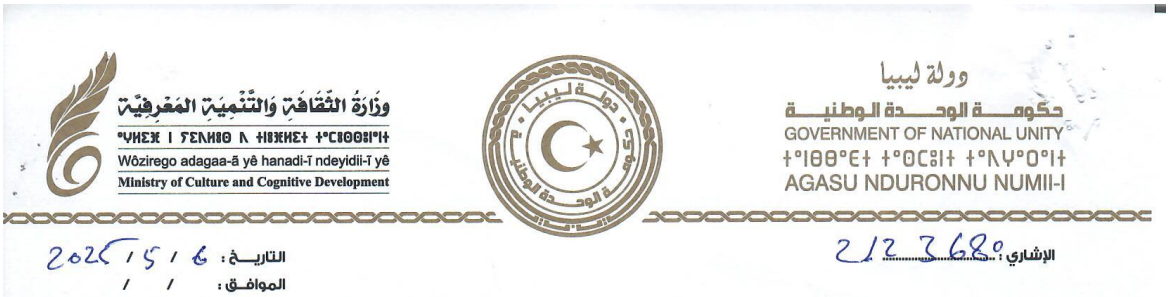
* المفاهيم والمصطلحات الرقمية والمستجدات التقنية.
* القوانين والتشريعات الوطنية والدولية المتعلقة بجرائم العالم الافتراضي والدليل الرقمي، واستعراض الفقه الدولي في هذا المجال.
* الإجراءات الأمنية والوقائية لمكافحة الجرائم الرقمية.
* القضايا التقنية والتحليلية المرتبطة بالعالم الافتراضي.

وتستهدف المجلة مختلف شرائح المجتمع، وبالأخص:

* المتخصصين في التقنية وأمن المعلومات.
* الأكاديميين والباحثين.
* أعضاء هيئة الشرطة والأجهزة الأمنية.
* أعضاء الهيئات القضائية.
* المهتمين بالتوعية المجتمعية في المجالات القانونية والتقنية.

كما تفتح المجلة أبوابها لاستقبال الأبحاث العلمية والمقالات المتخصصة التي تُسهم في إثراء المعرفة الرقمية، وتعزيز ثقافة الوعي بالقوانين والسياسات والإجراءات الأمنية في مواجهة التحديات والجرائم الافتراضية.

رئيس التحرير



القرار رقم (7) لسنة 2025م بشأن الإذن بإصدار مجلة علمية الكترونية

إدارة المطبوعـــــات والمصنفات الفنيـــة

- ❖ بعد الاطلاع على الإعلان الدستوري بتاريخ 2011/08/03م وتعديلاته .
- ❖ وعلى مخرجات الحوار السياسي المنعقد بتاريخ 9 نوفمبر 2020م .
- ❖ وعلي الاتفاق السياسي الموقع بتاريخ : 17 ديسمبر 2015 م .
- ❖ وعلى قانون النظام المالي للدولة الليبية ولائحة الميزانية والحسابات والمخازن وتعديلاتهما .
- ❖ وعلى القانون رقم (76) لسنة 1972م ، بشان إصدار قانون المطبوعات .
- ❖ وعلى القانون رقم (12) لسنة 2010 م ، بشأن تنظيم علاقات العمل ولائحته .
- ❖ وعلي ما قرره مجلس النواب الليبي في جلسته المنعقدة بتاريخ 10 مارس 2021 في مدينة سرت بشان منح الثقة لحكومة الوحدة الوطنية .
- ❖ وعلي قرار مجلس الوزراء رقم (299) لسنة 2021م ، بشأن اعتماد الهيكل التنظيمي لوزارة الثقافة والتنمية المعرفية .
- ❖ وعلى قرار وزير الثقافة والتنمية المعرفية رقم (156/ 2021) بشأن تكليف بمهام مدير إدارة المطبوعات والمصنفات الفنية .
- ❖ وعـلى كتـاب رئيس جهاز المباحث الجنائية بوزارة الداخلية بتـاريـخ 27-4-2025م رقـم إشـاري 6 .74/1838 والموجهـة إلى إدارة المطبوعات والمصنفات الفنية بشـأن الحصول عـلى إذن بإصـدار مجـلـة علميـة الكترونية - تحت اسـم (مجلة البوصلة الرقمية) .

info@culture.gov.ly +218 21 490 5325 +218 21 491 1955 +218 21 491 5519 ليبيا / طرابلس

دولة ليبيا
حكومة الوحدة الوطنية
GOVERNMENT OF NATIONAL UNITY
AGASU NDURONNU NUMII-I

وزارة الثقافة والتنمية المعرفية
Wôziregо adagaa-ā yê hanadi-ī ndeyidii-ī yê
Ministry of Culture and Cognitive Development

الإشاري : 2/2.36.80
التاريخ : 2025/5/6
الموافق : / /

- قـــرر -

مادة (1)

يـــؤذن لـرئـيـس جـهـاز المباحث الجنائية بإصـدار مجلـة علميـة تصـدر بصفـة (نـصف سنوية) تـحـت اسـم (مجلة البوصلة الرقمية) ومقرها / طرابلس وتتكـون هيئة التحريـر مـن السادة وهـم :

1- السيد- محمود عاشور العجيلي	رئيس مجلس إدارة	2 - السيد- صلاح الدين مصطفي محمد	رئيس هيئة التحرير
3- السيد- محمد عبد الرحمن الفيتوري	مدير التحرير	4 - السيد- عمر محمد بن يونس	عضـــواً
5- السيد- فرج بشير برنوص	عضـــواً	6 - السيد – أبوبكر محمد الهنشيري	عضـــواً

مادة (2)

يتحمّـل السيـد/رئيس هيئة التحرير المسئولية القانونية عما ينشر في (مجلة البوصلة الرقمية) والالتزام بما نص عليه قـانون المطبوعات رقم 76 لسنة 1972م .

مادة (3)

يتحمـّل رئيس جهاز المباحث الجنائية - النفقات والمصروفـات كـافـــة .

مادة (4)

تصدر المجلة في غضون ثلاثة أشهر من تاريخ صدور هذا القرار، وتبلغ إدارة المطبوعات والمصنفات الفنية بصورة من العقد الموقع مع الجهة الطابعة ، وتزويد الإدارة بعدد (5) نسخ من كل عدد يصدر عنها .

مادة (5)

يلغي القرار إذا لم تلتزم المجلة بتنفيذ ما نصت عليه المادة (4) من هذا القرار بمواعيد صدورها المحددة .

مادة (6)

يعمل بهذا القرار من تاريخ صدوره .

يوسـف رمضـــان موسى
مدير إدارة المطبوعات والمصنفات الفنية

صدر في طرابلس/
2025/5/5
بالتوفيق والنجاح

info@culture.gov.ly +218 21 490 5325 +218 21 491 1955 +218 21 491 5519 ليبيا / طرابلس

المحتويات

الافتتاحية

لواء محمود عاشور العجيلي
رئيس جهاز المباحث الجنائية
رئيس مجلس إدارة المجلة

"البوصلة الرقمية – العدد الثاني: من المتابعة إلى التمكين القانوني الرقمي"

بعد أن حظي العدد الأول من مجلة "البوصلة الرقمية" بمتابعة واسعة، واهتمام أكاديمي ومؤسسي لافت، واحتفاء من الباحثين والمتخصصين والفاعلين في المجال الأمني والقانوني والتقني، نعود اليوم لنواصل المسير بثقة ومسؤولية في إصدارنا الثاني، وقد تأكد لنا أن الحاجة إلى منبر علمي متخصص في قانون الإنترنت وأبعاده لم تعد خيارًا، بل ضرورة وطنية ومهنية واستراتيجية.

لقد أسس العدد الأول لمسار فكري جديد يعالج التحديات الرقمية من منظور قانوني تخصصي متكامل، وفتح الباب واسعًا أمام الحوار البنّاء حول الأطر التشريعية المنظمة للعالم الافتراضي، والتحديات المرتبطة بإنفاذ القانون في بيئة افتراضية تتسم بالتعقيد والديناميكية والتغير المستمر.

وفي هذا العدد الثاني، تمضي مجلة البوصلة الرقمية قُدمًا في تعزيز الوعي القانوني الرقمي، وتسليط الضوء على الجوانب التشريعية والجنائية والأمنية والأخلاقية المرتبطة باستخدام الإنترنت والتكنولوجيا الحديثة، في سياق تتزايد فيه الجرائم الافتراضية، وتتسارع فيه تطورات الذكاء الاصطناعي، وتشتد فيه الحاجة إلى مقاربات قانونية مرنة، حديثة، وفعالة.

نحن ندرك أن القانون لا يمكن أن يبقى جامدًا أمام متغيرات التقنية، كما أن الأمن لا يمكن أن يُبنى فقط على الأدوات دون فكر قانوني ووعي مجتمعي. ومن هنا، تلتزم المجلة بأن تكون منصةً بحثية رصينة، ومرجعية وطنية تخصصية، وفضاءً علميًا مفتوحًا للباحثين والخبراء والممارسين في مجال قانون الإنترنت ومكافحة الجريمة الرقمية.

إن إدارة مكافحة تقنية المعلومات بجهاز المباحث الجنائية، من خلال هذه المجلة، لا تسعى فقط للتوثيق أو التوعية، بل تعمل على بناء عقل قانوني رقمي جماعي، يعزز السيادة الرقمية الوطنية، ويدعم جهود الدولة في ترسيخ أمن العالم الافتراضي، ويواكب المنظومات القانونية الدولية.

ختامًا، نشكر كل من ساهم في إثراء محتوى العدد الأول، ونرحب بالمساهمين في هذا العدد الجديد، مؤمنين أن البوصلة قد اتجهت نحو الطريق الصحيح... ولن تتوقف.

مصطلحات رقمية

الهاكر Hacker:

وفق القضاء المقارن هو شخص لديه مهارات خاصة في مجال الحوسبة والرقمية وليس بمجرم.. وانما لا يعد الهاكر مجرم ما لم يرتكب جريمة منصوص عليها في قانون نافذ.

القرصان Pirate:

هو الشخص المرتكب لجرائم العدوان على الملكية الفكرية.. ومن الخطأ اطلاق هذا المصطلح على الهكرة..

الطرف الثالث third Party :

الطرف الثالث في قانون الانترنت هو دائما مزود الخدمة ISP.. سواء كان مزود اتصال او مزود خدمة بيانات... ويترتب على اعتراف القانون به كطرف ثالث العديد من الاثار القانونية. فهو ليس نقطة تواصل فقط كما تشير التقنية الى ذلك وانما له نظام قانوني متكامل.. بما في ذلك المسؤولية القانونية..

البنية التحتية للعالم الافتراضي Cyber Infrastructure

يشير مصطلح «البنية التحتية للعالم الافتراضي «Cyber Infrastructure» إلى موارد الاتصالات والتخزين والحوسبة التي تعمل عليها البيانات وأنظمة المعلومات.

التحريات عبر المصادر المفتوحة

إعداد :

لواء صلاح الدين مصطفى بن سليمان

مدير إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية

المهندس محمد بشير الأسير

عضو مكتب الطب الشرعي الرقمي

بإدارة مكافحة جرائم تقنية المعلومات

التحريات عبر المصادر المفتوحة (OSINT)

المفهوم: -

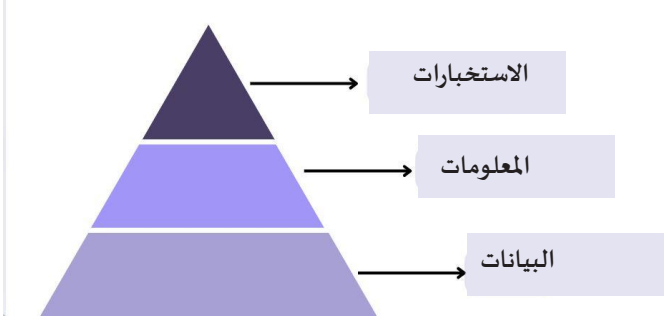
التحريات عبر المصادر المفتوحة (OSINT) هي عملية تحليل ومعالجة البيانات التي تم الحصول عليه بشكل قانوني من مصادر متاحة للعامة، بهدف إنتاج معرفة استخباراتية تدعم صناع القرار أو تحقق أهداف بحثية أو أمنية أو استراتيجية .يتم جمع هذه المعلومات من وسائل الإعلام التقليدية، ومنصات الإنترنت، وقواعد البيانات العامة، والوثائق الحكومية المنشورة، والمصادر الأكاديمية، ووسائل التواصل الاجتماعي، وغيرها من الموارد التي لا تتطلب وسائل سرية أو غير قانونية للوصول إليها.

مقارنة بين البيانات – المعلومات – الاستخبارات: -

البيانات: تشير البيانات إلى مجموعة من المعطيات الالوية غير المعالجة، والتي قد تكون في صورة ارقام أو نصوص أو رموز أو مشاهدات منفصلة، لا تحمل البيانات بمفردها دلالة واضحة ما لم يتم ترتيبها أو تفسيرها.

المعلومات: هي ناتج معالجة البيانات وتحليلها وتنظيمها بطريقة تصيف لها معنى وسياقا

الاستخبارات: هي عملية متقدمة تعتمد على جمع المعلومات المتنوعة، ثم تحليليها وربطها بسياق محدد لإنتاج معرفة معمقة تستخدم لدعم عمليات صنع القرار الاستراتيجي أو الأمني أو الاقتصادي.



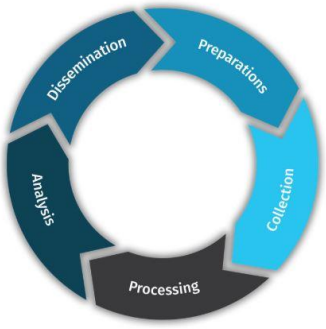
تاريخ التحريات عبر المصادر المفتوحة (OSINT):

بدأت أصول ال OSINT خلال الحرب العالمية الثانية، حيث أنشأت منظمات مثل BBC Mentoring وFBMS لرصد وتحليل البث الإذاعي الأجنبي، مما وفر للحلفاء معلومات مهمة عن خطط العدو ودعايته.

بعد الحرب تراجع الاهتمام بال OSINT مقارنة بالأنواع الاستخبارات الأخرى مثل العمليات السرية، ومع ذلك أعاد انتشار الإنترنت ووسائل الاتصال الرقمية الاهتمام بها من جديد حيث لعبت وسائل التواصل الاجتماعي دورا أساسيا في جمع المعلومات وتنسيق أبرز الأحداث العالمية الأخيرة، مما برز قوة OSINT في العصر الرقمي.

خطوات التحريات عبر المصادر المفتوحة (OSINT)

- التحضير / دراسة ومعرفة الهدف لتحديد الاسلوب والاداة المناسبة.
- الجمع / جمع كافة البيانات المتاحة.
- التقييم والمعالجة / معالجة البيانات المجمعة للحصول على معلومات
- التحليل والتصنيف / تحليل المعلومات بعد المعالجة للوصول الى نتائج ربط العلاقات بين ما تم جمعه من معلومات وكيانات واشخاص والخروج بمنتج معلوماتي يساعد في اتخاذ القرارات وتحقيق الاهداف.
- النشر والمشاركة مع جهات الاختصاص والجهات الطالبة .



مصادر جمع البيانات:

الشبكة العالمية: المواقع الالكترونية المتاحة على الشبكة للجميع والمعلومات والمنتديات وشبكات التواصل الاجتماعي بكافة تطبيقاتها وكذلك البرامج المتاحة للعامة والخرائط الجغرافية الالكترونية وغيرها.

الاعلام: المرئي - المسموع - المطبوع (الصحف والمجلات والنشرات الدولية).

البيانات الحكومية العامة: وهي البيانات التي تنشرها الحكومة أو من خلال الخطابات الرسمية والمؤتمرات الصحفية وغيرها.

قواعد البيانات: التي تم نشرها او تسريبها

المنتديات: المجموعات المفتوحة

مستويات التحريات عبر المصادر المفتوحة(OSINT LEVELS) :

المستوى الأول: جمع معلومات متاحة وواضحة للعامة وتتطلب مهارة تقنية بسيطة.

- البحث في Google أو Bing.
- قراءة الأخبار المنشورة.
- الاطلاع على الملفات الشخصية العلنية (مثلLinkedIn ، فيسبوك)

المستوى الثاني: جمع معلومات قد تكون متاحة، لكن تحتاج إلى بعض التقنيات والمهارات للوصول إليها وتحليلها.

- استخدام أدوات متخصصة لتحليل الشبكات الاجتماعية (مثل Maltego).
- استخراج بيانات مخفية في الصور
- البحث في الأرشيفات مثل Wayback Machine.
- تحليل الخرائط والصور الجوية

المستوى الثالث: اجراء عمليات بحث معقدة جدا على المصادر المفتوحة ولكن بطريقة ذكية وشاملة، تضمن الربط بين معلومات متفرقة وتحليلها لاستخلاص استنتاجات حساسة.

- استخدام الذكاء الاصطناعي أو تقنيات البيانات الضخمة لتحليل كميات هائلة من المعلومات المفتوحة.
- تتبع تحركات الأفراد عبر أدوات تعقب الرحلات البحرية والجوية والسجلات العامة.
- اكتشاف البنية التحتية الرقمية للشركات

التحريات عبر المصادر المفتوحة من حيث النشاط

- **التحريات عبر المصادر المفتوحة السلبية:**

السلبية تعني أنك لا تتفاعل مع الهدف. يُعرّف الجمع السلبي للمصادر المفتوحة بأنه جمع المعلومات عن هدف معيّن باستخدام المعلومات المتاحة للعامة. السلبية تعني أنه لن يكون هناك أي تواصل أو تفاعل مع الأفراد عبر الإنترنت، بما يشمل التعليق أو المراسلة أو إرسال طلبات صداقة أو المتابعة.

- **التحريات عبر المصادر المفتوحة النشطة:**

النشاط يعني أنك تتفاعل مع الهدف بطريقة ما، مثل إضافة الهدف كصديق على الملفات الشخصية في وسائل التواصل الاجتماعي، أو الإعجاب بمنشوراته، أو التعليق عليها، أو مراسلته، وما إلى ذلك. يُعتبر البحث النشط باستخدام المصادر المفتوحة نوعًا من التفاعل،

مقارنة التحريات عبر المصادر المفتوحة بين السلبية والنشطة:

التحريات مفتوحة المصدر السلبية	التحريات مفتوحة المصدر النشطة
عدم التفاعل مع الهدف	التفاعل مع الهدف
جمع المعلومات بشكل سلبي من المصادر المتاحة للعامة	قد يتطلب الحصول على إذن خاص
انخفاض خطر التعرف على هوية القائم بالجمع	ارتفاع خطر التعرف على هوية القائم بالجمع

مستخدمو التحريات عبر المصادر المفتوحة (OSINT)

الحكومات – أجهزة أنفاذ القانون – القوات العسكرية – الصحفيون الاستقصائيون – محققو حقوق الانسان – مكاتب المحماة – أمن المعلومات – استخبارات التهديدات السيبرانية – مختبرو الاختراق – مهندسو الهندسة الاجتماعية.

جوانب استخدام التحريات عبر المصادر المفتوحة:

- **جوانب الأمن والاستخبارات**: يمكن استخدام الاستخبارات مفتوحة المصدر لجمع معلومات عن التهديدات الأمنية المحتملة، مثل الأنشطة الإرهابية أو الجريمة المنظمة العابرة للوطنية او الهجمات السيبرانية .
- **الأعمال التجارية وبحوث السوق**: يمكن استخدام الاستخبارات مفتوحة المصدر لجمع معلومات عن المنافسين، واتجاهات الصناعة، وسلوك المستهلكين.
- **الصحافة الاستقصائية**: يمكن للصحفيين الاستقصائيين استخدام الاستخبارات مفتوحة المصدر لجمع المعلومات حول مجموعة متنوعة من المواضيع.
- **البحوث الأكاديمية**: يمكن للباحثين استخدام الاستخبارات مفتوحة المصدر لجمع البيانات حول موضوعات متعددة.
- **الإجراءات القانونية**: يمكن استخدام الاستخبارات مفتوحة المصدر في الإجراءات القانونية لجمع الأدلة أو لإجراء التحريات اللازمة عن الشهود المحتملين أو المدعى عليهم.

مزايا التحريات عبر المصادر المفتوحة (OSINT)

- **الوصول إلى المعلومات المتاحة للعامة:** تجمع الاستخبارات مفتوحة المصدر المعلومات المتاحة علنًا والقابلة للوصول قانونيًا.
- **مجموعة واسعة من المصادر:** يمكن جمع الاستخبارات مفتوحة المصدر من مجموعة واسعة من المصادر،
- **التوقيت:** نظرًا لأن الاستخبارات مفتوحة المصدر تعتمد على المعلومات المتاحة علنًا، يمكن جمعها بسرعة وفي الوقت الفعلي .
- **الفعالية من حيث التكلفة:** تعتبر الاستخبارات مفتوحة المصدر أكثر فعالية من حيث التكلفة مقارنةً بطرق جمع الاستخبارات الأخرى.
- **الشفافية:** الاستخبارات مفتوحة المصدر شفافة ويمكن التحقق منها بسهولة .

أهمية التحريات عبر المصادر المفتوحة لجهات انفاذ القانون:

1- الوصول إلى معلومات ضخمة ومنوعة:

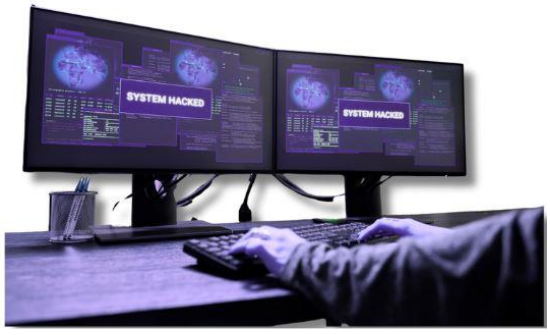
- وسائل التواصل الاجتماعي
- المنتديات العامة
- المواقع الإخبارية
- قواعد البيانات المفتوحة
- السجلات الرسمية المتاحة

2- **الكشف المبكر عن التهديدات:**

- التخطيط لهجمات إرهابية أو أعمال شغب
- الترويج للجرائم عبر الإنترنت
- متابعة الحسابات المتطرفة
- نشاطات مشبوهة على السوشل ميديا
- مراقبة الهجمات السيبرانية

3- **دعم التحقيقات الجنائية:**

- تتبع الأفراد وتحركاتهم الرقمية
- الربط بين الأشخاص والمجموعات
- تحليل أنماط السلوك أو العلاقات
- تتبع المعاملات والانشطة المالية



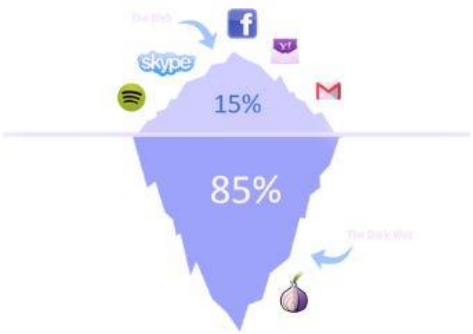
أنواع التحريات عبر المصادر المفتوحة (OSINT)

1- الاستخبارات من وسائل التواصل الاجتماعي (SOCMINT):

تركز الاستخبارات من وسائل التواصل الاجتماعي (SOCMINT) على جمع وتحليل البيانات من منصات وسائل التواصل الاجتماعي مثل فيسبوك، وتويتر، ولينكدإن وغيرها. تُعد هذه النوعية من الاستخبارات قيمة لفهم الأنشطة في الوقت الفعلي، وربط وفهم العلاقات والكيانات.

2- استخبارات الويب المظلم (DARKINT):

تتضمن الاستخبارات من الويب المظلم (DARKINT) الوصول إلى المعلومات وتحليل البيانات من الويب المظلم، وهو جزء من الإنترنت لا يتم فهرسته بواسطة محركات البحث التقليدية ويتطلب برامج متخصصة مثل Tor للوصول إليه. يعد الويب المظلم مركزًا للأنشطة غير القانونية، مما يجعله مصدرًا مهمًا للاستخبارات حول الشبكات الإجرامية، والتجارة غير القانونية، وتهديدات الأمن السيبراني .

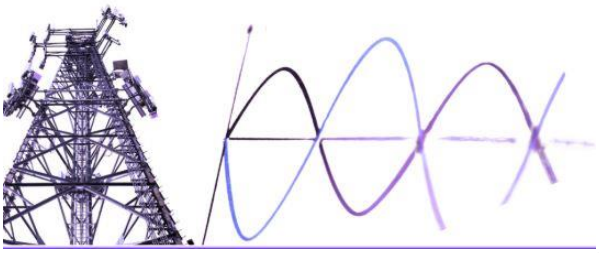


3- الاستخبارات الجغرافية المكانية (GEOINT):

تستخدم الاستخبارات الجغرافية المكانية (GEOINT) صور الأقمار الصناعية وبيانات جغرافية أخرى لجمع المعلومات حول المواقع والأحداث الجغرافية. تُعد GEOINT قيمة للعمليات العسكرية والأمنية، ورصد البيئة، والاستجابة للكوارث، وتخطيط المدن وغيرها من الاستخدامات المهمة.

4- استخبارات الإشارات عبر المصادر المفتوحة (SIGINT)

وهي جمع المعلومات وتتبع وتحليل الإشارات اللاسلكية أو الاتصالات التقنية التي تكون متاحة بشكل علني للعامة، دون الحاجة لاختراق أو تجسس مباشر. الفكرة الأساسية تقوم على مراقبة البيانات التي تُبث أو تُرسل عبر شبكات غير مشفّرة أو التي تُنشر بشكل طوعي من قبل الأفراد أو المؤسسات، مثل الاتصالات اللاسلكية العامة، إشارات الأقمار الصناعية المفتوحة، أو بث الراديو غير المشفر وكذلك إشارات الرادارات والكاميرات الحرارية،



5- الاستخبارات المالية عبر المصادر المفتوحة (FININT)

تركز على جمع وتحليل المعلومات المتعلقة بالأموال والمعاملات المالية من مصادر علنية وغير سرية بهدف تتبع الأنشطة المالية المشبوهة، أو تحليل السلوك الاقتصادي لكيانات أو أفراد، أو دعم التحقيقات في قضايا مثل غسل الأموال، الفساد، أو تمويل الإرهاب.

6- الاستخبارات السيبرانية (CYBINT)

هي عملية جمع وتحليل المعلومات المتعلقة بالفضاء الإلكتروني، بهدف الكشف عن التهديدات الأمنية، الهجمات السيبرانية، أو النشاطات الرقمية الخبيثة، سواء كانت صادرة عن أفراد، جماعات، أو دول. تعتمد CYBINT على تتبع أنشطة الهاكرز، البرمجيات الخبيثة، الشبكات المظلمة - والمنتديات الخاصة.

التحديات التي تواجه التحريات عبر المصادر المفتوحة:

فرط البيانات والإيجابيات الكاذبة: جمع البيانات من مصادر متعددة يؤدي إلى تراكم كميات هائلة من المعلومات مما يخفي المعلومات المهمة ويتخللها العديد من المعلومات المضللة.

الحدود الأخلاقية والقانونية: جمع المعلومات من المجال العام قد ينتهك أحيانًا حق الخصوصية أو يتحول إلى ممارسة أشبه (كشف معلومات شخصية عن الأفراد).

تطور المنصات والانماط الرقمية بسرعة: كالانتقال من المنتديات المفتوحة إلى التطبيقات المشفّرة أو الاستفادة من الخصوصية التي توفرها وسائل التواصل الاجتماعي والعملات المشفرة والانترنت المظلم وغيرها.

التحقق من المصادر وموثوقيتها: ليست كل البيانات المفتوحة موثوقة — فبعضها قد يكون شائعات، أو لقطات شاشة مزيفة، أو معلومات مغلوطة. الاعتماد المفرط على بيانات غير مؤكدة قد يؤدي إلى استنتاجات خاطئة أو إهدار الموارد.

أفضل أداء في التحريات عبر المصادر المفتوحة (OSINT) تتم عبر الخطوات التالية:

حدد هدفك: يجب ان تحدد الهدف وراء استخدامك للاستخبارات مفتوحة المصدر إذا تريد بحث عن معلومات عن شخص ما او مجموعة ما او انتهاكات لحقوق العلامة التجارية من المهم وضع حدود واضحة للبحث لتجنب إضاعة الوقت في معالجة بيانات غير ذات صلة.

اختيار الأدوات والمنهجيات المناسبة: ينبغي اختيار أدوات جمع المعلومات المفتوحة المصدر بما يتناسب مع الهدف المحدد، مثل استخدام أدوات البحث عن الأسماء للبحث عن الأفراد، أو الاستعانة ببرامج متخصصة في البحث عن الصور لتحليل الصور الرقمية، أو توظيف أدوات البحث الجغرافية للحصول على معلومات مكانية دقيقة.

الالتزام بالمعايير الأخلاقية والقانونية: لضمان أن العمل قد لا ينخرط في عمل غير قانوني او انتهاك لحقوق الخصوصية.

التحقق والتقاطع مع مصادر متعددة: لا تعتمد على منشور واحد أو مصدر ادعاء فردي — بل تحقق من عدة مصادر مختلفة ويجب أن تكون متشابهة أو داعمة لبعضها البعض.

دور الذكاء الاصطناعي في التحريات عبر المصادر المفتوحة (AI-OSINT):

- **تحسين مرحلة جمع البيانات:** عبر تصفية المعلومات وترتيب البيانات حسب الأولوية.
- **تحسين مرحلة تحليل البيانات:** من خلال ربط المعلومات ذات الصلة واكتشاف البنية المفيدة ضمن البيانات.
- **تعزيز الرؤى القابلة للتنفيذ:** حيث يستطيع تحليل الذكاء الاصطناعي مراجعة كميات ضخمة من البيانات الخام تفوق قدرة المحللين البشر، مما يسمح باستخلاص رؤى أكثر دقة وقابلية للتنفيذ من المعلومات المتاحة

أساليب حماية مستخدمي التحريات عبر المصادر المفتوحة (OSINT):

1- التصفح المجهول :

استخدام متصفح ضد التعقب مثل تطبيق BRAVE الذي صمم للأغراض الخصوصية.

رابط التنزيل https://laptop-updates.brave.com/download/BRV010?bitness=64

2- التصفح المجهول:

استخدام محرك بحث مثل DuckDuckGO الذي يوفر تجربة البحث في الانترنت بطريقة أمنة.

رابط محرك البحث: https://duckduckgo.com

3- التصفح المجهول:

استخدام اضافة uBlock Origin وهي مفتوحة المصدر تستخدم أدوات عدم التتبع والتحقق من المواقع الضارة، وقفل النوافذ المنبثقة(Pop-ups)

رابط التنزيل: https://ublockorigin.com

4- التصفح المجهول:

استخدام الشبكات الافتراضية الخاصة (VPNS) مثل بروتون.

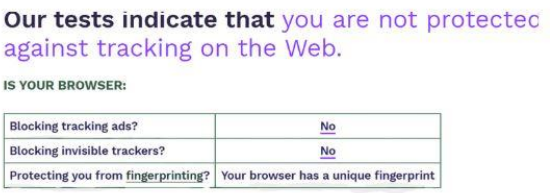
برنامج بروتون يتيح لك استخدام VPN مجاني لحماية خصوصيتك.

رابط تنزيل برنامج بروتون: https://protonvpn.com/download

5- التصفح المجهول:

استخدام موقع coveryourtracks للتأكد من أن المتصفح الذي تستخدمه محمي بشكل جيد. حيث ان هذا الموقع يقوم باختبار مدى حماية المتصفح الذي تستخدمه في الانترنت.

رابط الموقع: https://coveryourtracks.eff.org


Our tests indicate that you are not protectec against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	No
Blocking invisible trackers?	No
Protecting you from fingerprinting?	Your browser has a unique fingerprint

6- تعزيز السلامة المعلوماتية:

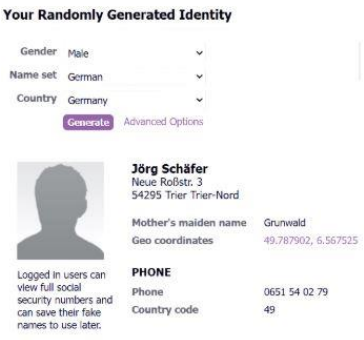
يُستحسن في سياق الأعمال الفنية والاستدلالات الجنائية عبر الانترنت، مراعاة الفصل بين الوسائل المستخدمة في المهام الاعتيادية وتلك المعنية بمهام الرصد والتتبع، وذلك تجنّبًا لأي تقاطع قد يؤثر على سلامة الإجراءات أو يحد من فاعليتها.

7- البحث الأمن في وسائل التواصل الاجتماعي:

استخدم هوية رقمية مستعارة للتحري في وسائل التواصل الاجتماعي.

استخدم موقع fakenamegenerator لأنشاء هوية رقمية مستعارة.

رابط الموقع: https://fakenamegenerator.com


Your Randomly Generated Identity

Gender Male
Name set German
Country Germany
Generate Advanced Options

Jörg Schäfer
Neue Roßstr. 3
54295 Trier Trier-Nord

Mother's maiden name Grunwald
Geo coordinates 49.787902, 6.567525

PHONE
Phone 0651 54 02 79
Country code 49

Logged in users can view full social security numbers and can save their fake names to use later.

8- البحث الأمن في وسائل التواصل الاجتماعي:

يمكنك أيضا انشاء صورة خاصة بك لجعل الهوية المستعارة الخاصة بك أكثر صدقا

موقع thispersondoesnotexist يتيح لك انشاء صورة لشخص بواسطة الذكاء الاصطناعي غير موجود في الحقيقة.

رابط الموقع: https://www.thispersondoesnotexist.cc

9- حماية نظام تشغيل المستخدم:

استخدم برامج مكافحة الفيروسات والجدران النارية المحدثة، وحافظ على تحديث أنظمة التشغيل والتطبيقات لسد الثغرات.

قم بتنزيل Bitdefender وهو برنامج حماية مجاني وقم بتفعيله للجهاز الخاص بك

رابط التنزيل: https://www.bitdefender.com/en-us/consumer/free-antivirus

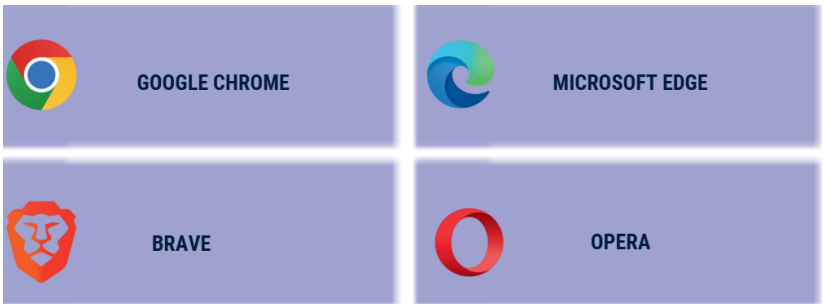
10- حماية نظام تشغيل المستخدم:

استخدم كلمات مرور قوية لنظام التشغيل والحسابات الخاصة بك.

- اجعل كلمات المرور تتكون من خليط من حروف كبيرة وصغير مع رموز وارقام.
- استخدم برنامج KeePassXC لحفظ وتنظيم كلمات السر الخاص بك في مكان واحد وبسرية تامة.
- رابط التنزيل: https://keepassxc.org/download

تقنيات التحريات عبر المصادر المفتوحة:

1- المتصفح (browser): هو برنامج تطبيقي يستخدم لعرض صفحات الويب والوصول إلى المحتويات عبر الانترنت.

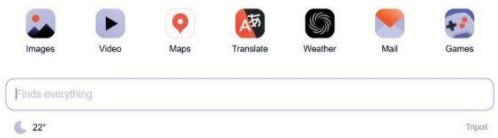


2-محركات البحث: محركات البحث أداة محورية في عمليات جمع المعلومات المفتوحة المصدر (OSINT)، إذ تتيح للمحللين الوصول إلى بيانات واسعة النطاق بسرعة وكفاءة، مما يعزز من دقة التحليل وسرعة اتخاذ القرار.

محرك البحث	السنة
Archie	1990
WebCrawler	1994
Lycos	1994
Yahoo!	1994
Google	1998
Bing	2009
DuckDuckGo	2008

3- محرك بحث YANDEX: من أفضل محركات البحث في الحصول على المعلومات في الانترنت خصوصا تلك التي لا تظهر في نتائج قوقل وبينق، ويوفر أيضا خدمة البحث عن الصور والخرائط الجوية.

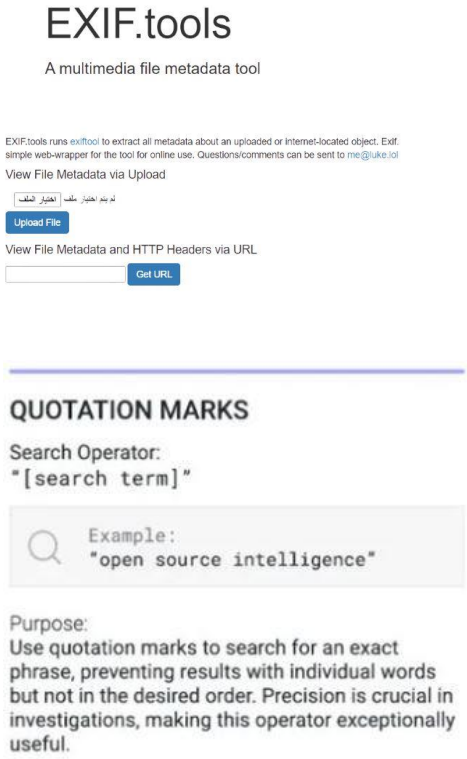
Yandex

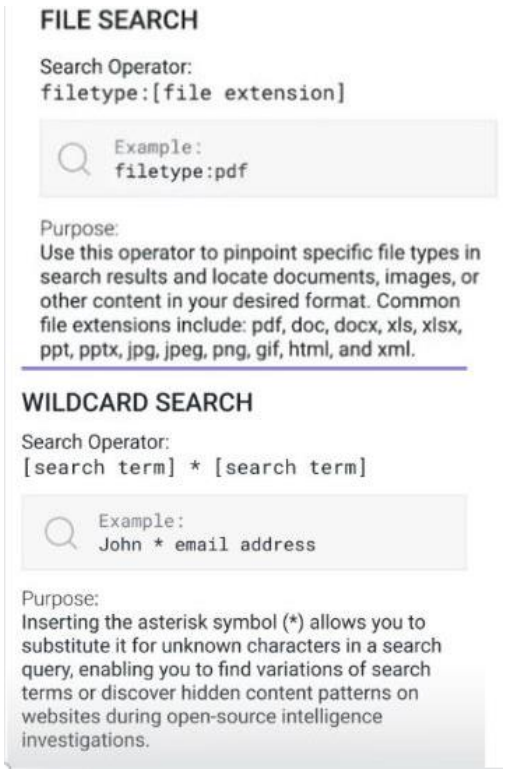


4- جوجل دوركس (google dorks): هي تقنية متقدمة في مجال جمع المعلومات مفتوحة المصدر (OSINT)تعتمد على استخدام أوامر بحث خاصة ضمن محرك بحث جوجل للوصول إلى معلومات قد لا تكون ظاهرة للمستخدمين العاديين.

- site: لتحديد نتائج البحث ضمن موقع معين
- filetype: PDF أو DOC للبحث عن ملفات بنوع معين مثل.
- inurl: URL للعثور على صفحات تحتوي على كلمات محددة في عنوان.
- intitle: للبحث عن صفحات تحتوي على كلمات معينة في عنوان الصفحة.
- intext: للبحث عن كلمات داخل محتوى الصفحة

5- استخراج البيانات الوصفية EXIF: يمكن أن تحتوي الصور أو المستندات أو ملفات PDF على بيانات وصفية مثل الطوابع الزمنية أو الموقع الجغرافي أو معلومات الجهاز أو معلومات المالك.





6- البحث في وسائل التواصل الاجتماعي: هي برامج أو منصات تساعد في جمع والبحث على حسابات وسائل التواصل مثل تويتر، فيسبوك، إنستغرام، ولينكد إن.

- استخدم IDcrawl للبحث عن الحسابات **https://www.idcrawl.com**
- استخدم social-searcher للبحث عن الحسابات: **https://www.social-searcher.com**
- استخدم INFOSPACE للبحث عن الحسابات: **https://infospace.com**
- استخدم USERSEARCH للبحث عن الحسابات: **https://www.usersearch.org**
- استخدم Instant Username Searchللبحث عن الحسابات:
  https://instantusername.com

7- البحث في الخرائط الجوية:

هو استخدام أدوات وتقنيات تعتمد على بيانات الأقمار الصناعية أو خدمات الخرائط الرقمية مثل Google Mapsأو Google Earth لتحليل المواقع الجغرافية وتحديد الأنشطة أو البنية التحتية أو التغيرات في الأماكن.

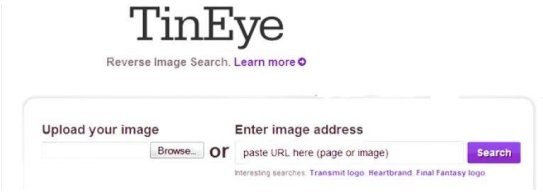
استخدم Google Earth للحصول:// على صور جوية ذات دقة عالية

رابط الموقع: **http:searth.google.com**

8- البحث العكسي عن الصور:

البحث العكسي عن الصور هو تقنية تتيح للمستخدمين تحميل صورة أو إدخال رابط صورة من الإنترنت للعثور على صور مشابهة أو مطابقة لها على الويب، استخدم برنامج tineye للبحث عن الصور.

رابط الموقع: **https://tineye.com**



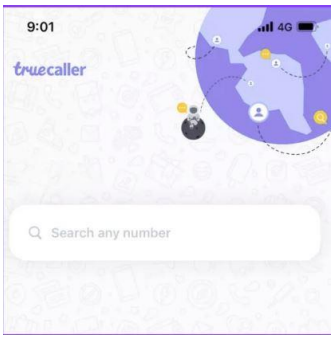
9- البحث العكسي عن الصور:

البحث العكسي عن الصور هو تقنية تتيح للمستخدمين تحميل صورة أو إدخال رابط صورة من الإنترنت للعثور على صور مشابهة أو مطابقة لها على الويب، استخدم برنامج facecheck للبحث عن الصور.

رابط الموقع: **https://facecheck.id**

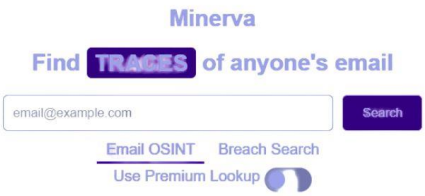
10- البحث عن أرقام الهواتف: قد ترتبط حسابات وسائل التواصل الاجتماعي، أو بيانات تم تسريبها من قبل شركات سبق لها التعامل مع هؤلاء الأشخاص، استخدم برنامج truecaller للبحث عن الأرقام.

رابط الموقع: https://www.truecaller.com



11- البحث عن البريد الالكتروني: لتحديد وجود او صحة بريد إلكتروني معين، او لجمع معلومات مرتبطة به مثل الهوية، او الحسابات المرتبطة، استخدم موقع minervaosint للبحث عن معلومات حول البريد الالكتروني.

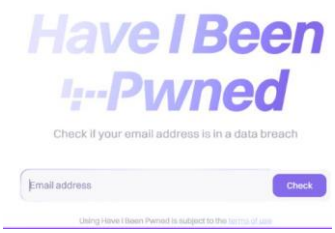
رابط الموقع: https://minervaosint.com



12- البحث عن البريد الالكتروني:

في بعض الاحيان قد يتم العثور على معلومات تخص البريد الالكتروني في قواعد البيانات المسربة، استخدم موقع haveibeenpwned للبحث في قواعد البيانات.

رابط الموقع: https://haveibeenpwned.com



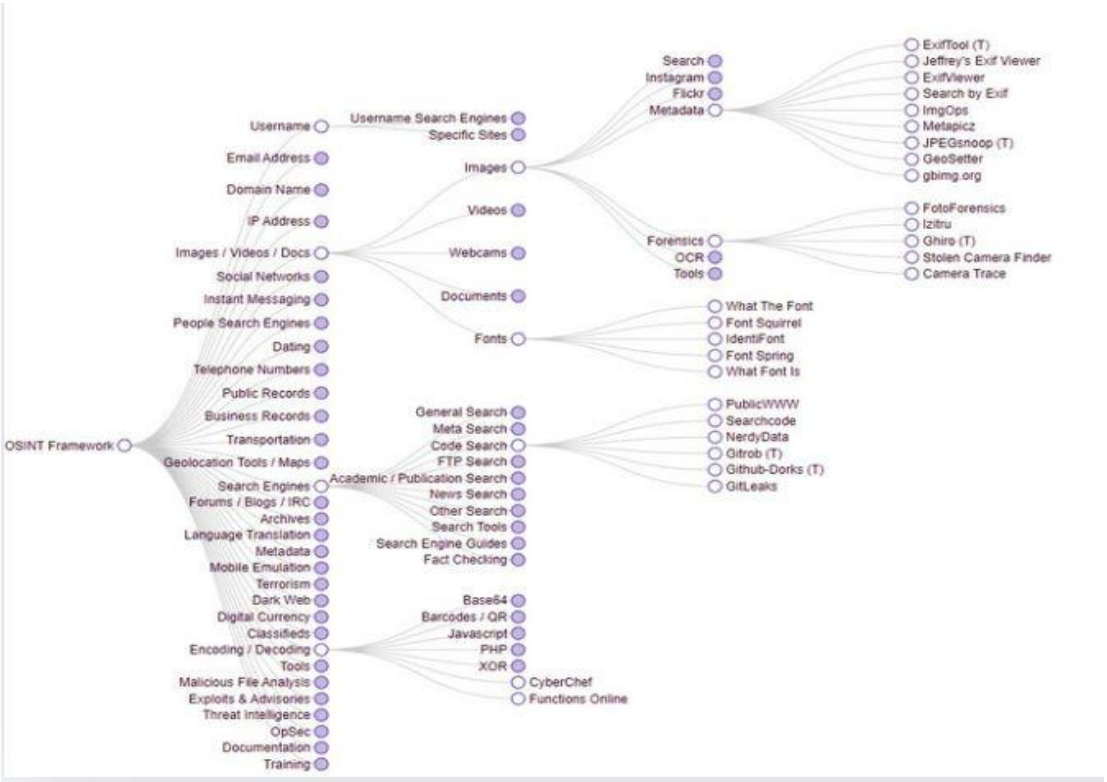
13- **البحث في العملات المشفرة:** جمع وتحليل المعلومات المرتبطة بالعملات الرقمية بهدف فهم حركة الأموال الرقمية، وكشف الأنشطة غير المشروعة، أو ربط المحافظ المشفرة بهويات حقيقية، استخدم موقع intel arkham للبحث في سجل معاملات العملات الرقمية المشفرة.

رابط الموقع: **https://intel.arkham.com**

Arkham

14- OSINT frame work :مجموعة شاملة من الادوات والموارد المصممة بطريقة تساعد المحللين في البحث وجمع وتنظيم المعلومات مفتوحة المصدر.

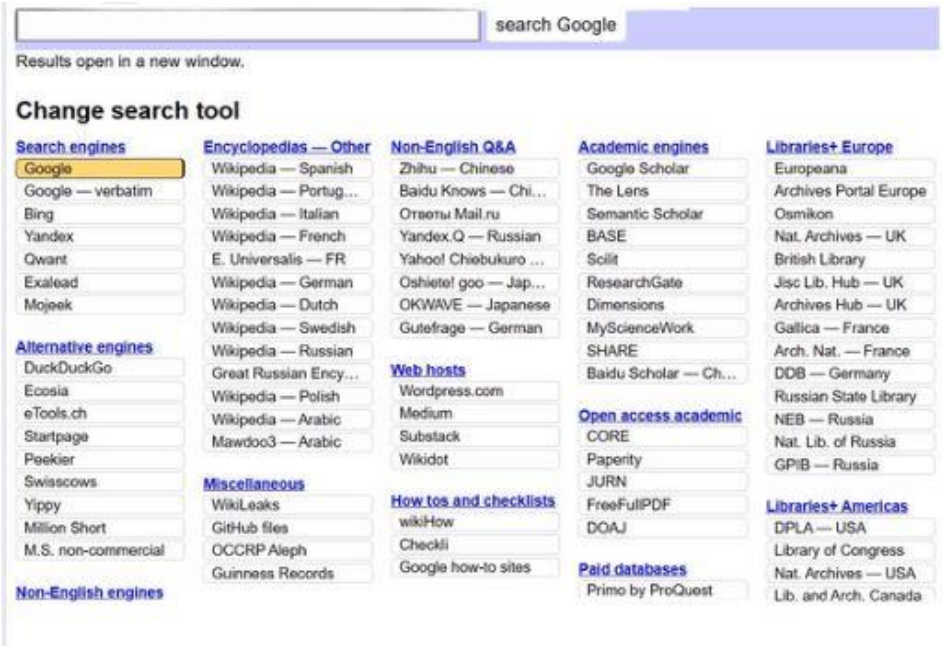
رابط الموقع: https://osintframework.com



15- Fagan Finder:

أداة لتجميع محركات البحث في مجال جمع المعلومات مفتوحة المصدر (OSINT) ، حيث يوّفر واجهة موحدة تتيح للمستخدمين الوصول إلى العديد من محركات البحث وقواعد البيانات المختلفة.

رابط الموقع: https://faganfinder.com



16- OSINT Rocks:

وهي مجموعة من الادوات الي توفر لك خدمة البحث عن اسماء مستخدمين وارقام هواتف والبريد الالكتروني.

رابط الموقع https://osint.rocks

osint.rocks

أمثلة واقعية على استخدام التحريات عبر المصادر المفتوحة (OSINT):

1- **دور فيسبوك في قضايا الاحتيال والاشخاص المفقودين:** في إحدى العمليات، استخدم المحققون تقنيات OSINT المتعلقة بحسابات فيسبوك لحل قضايا أشخاص مفقودين. ومن خلال تحليل بيانات Marketplace Facebook ونشاطات المستخدمين، تمكنوا من تحديد آخر المواقع المعروفة وبناء تصورات رقمية Digital personas عن الافراد المستهدفين.

للاطلاع على مزيد من التفاصيل

https://www.osint.industries/project/using

facebook-to-crack-fraud-and-find-missing-persons-with-osinttactical

2- **كشف خداع العملات الرقمية:** استخدم الباحثون أطر عمل OSINT مدمجة مع تحليلات البلوك تشين لتحديد منفذ عملية احتيال في العملات الرقمية، والذي كان يتواصل مع الضحايا مباشرة عبر تطبيقات مثل واتساب، والبريد الإلكتروني، والتيليغرام .استطاع التحقيق تتبع أسلوب الجناة من خلال تحليل البصمات الرقمية والمعاملات على شبكة البلوك تشين، دون الحاجة للاعتماد على منشورات المنتديات أو مشاركة المستخدمين.

الإثبات الجنائي عبر الإنترنت

إعداد

د. عمر محمد بن يونس

مستشار موسوعة التشريعات العربية

(جينيس للأرقام القياسية 1999 – كتاب 2002 – ص. 156)

رئيس الجمعية العربية لقانون الإنترنت

أنتجت حالة الصـــراع بين المجتمع والجريمة في ثوبها الجديد– الناجمة عن اســتخدام الانترنت- نظرة جديدة الى الإثبات الجنائي، تمثلت في ســـؤال فرض نفســـه على دراســـات القانون الجنائي، يتناول في موضوعه البحث في مدى إمكانية تجاوب وسائل الإثبات الجنائي التقليدية مع التقنية الجديدة للانترنت.

وهذا التســـاؤل يقود في الحقيقة الى الإقرار بأن ظاهرة جديدة برزت لتنضـــم بجدارة الى المفاهيم التقليدية للدليل، وهي هنا الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاســـوب والانترنت، بحيث يصـــح أن يطلق على الارتباط بين الظاهرة الرقمية الجديدة وبين الاثبات الجنائي تســـمية جديدة للدليل هي الدليل الرقمي Digital evidence او الدليل الالكتروني Electronic evidence حسـبما أطلق عليه المشـرع الاوروبي[1] والمقارن هذا المصـطلح. سـيما وقد اعتدت به المحاكم في النظم القانونية المقارنة، سـواء من حيث جدواه او من حيث قيمته القانونية، فتم إحداث تسوية شبه منطقية بينه وبين الدليل الجاري او التقليدي المتعارف عليه، والمستمد من وسائل الحصول عليه المعروفة، كالتلبس والتفتيش والشهادة والقرائن وأيضا الاعتراف، ولتصـبح له فيما بعد الحظوة التي يحظى بها الآن. وأسـاس هذه التسـوية المنطقية هنا هي نظرة الى الواقع الجدي للتقنية الرقمية لكونها ذات مدلول مؤثر وحقيقي في عالم الانسـان المعاصـر والمسـتقبلي، فما تنتجه التقنية الرقمية يؤدي دورا لا يمكن تجاهله حتى في المجتمعات التي يعد نمو ها بطيئا في هذا المجال.

وإذا كان القضـاء المقارن قد أسـهم بدوره في تكوين معالم الدليل الرقمي – بمجرد قبوله له ليكون مصـدرا يلهم قاضـــي الإدانة كما البراءة في أحكامه - فإن ذلك في الحقيقة لا يمنع من التقرير بأن علماء التقنية كان لهم الدور المؤثر هنا. ومثل هذا الامر ســوف يقود الى بحث نظم الخبرة ومدى تأثيرها على قناعة قاضـــي الموضوع.

ســوف نتولى هنا التعرض لموضـــوع الدليل التقني، فنعرض لمحاولة تعريفه وأنواعه في فصـــل أول، ثم نتناول في فصل ثان موضوع الخبرة التقنية.

[1] **UC , Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies) Available on line in dec. 2000 at http://www.usdoj.gov/criminal/cybercrime/crycoe.htm**

الفصل الأول
الدليل الرقمي

أن البحث في نطاق الدليل الرقمي يجعل الباحث - وبحق - عرضة لخضم هائل من الآراء التقنية تردد هذا المصطلح، في الوقت الذي تشتبه عليه الأساليب - وليس المعايير - التي يتم الاستناد اليها في رصد هذا الدليل، حتى إنه من الصعوبة بمكان رصد وجود أسلوب محدد يمكن أن يقدم ولو جزئيا منطقا قانونيا يمكن من خلاله رصد ذلك المعيار المفقود للدليل الرقمي. ولعل مثار الصعوبة هنا يكمن في عدم الاستقرار القانوني في كيفية التعامل مع الدليل الرقمي، حتى مع قبول القانون واعترافه بهذا الدليل فإن عملية إقراره والاعتماد عليه تجعل عملية بحث موضوعه وأنواعه تزداد صعوبة، سيما إذا أدركنا إن مصطلح الدليل الرقمي يوجد له منزلة مختلفة عن تلك المنزلة التي يكون عليها الدليل المادي. فالتصنيف الذي عليه الدليل المادي إنما يعد -الآن- تصنيفا مقننا يجد له موضعا في القانون ويمكن الاستناد إليه، او الى أحد أنواعه المحددة في بناء الإدانة الجنائية. أما الدليل الرقمي فإن التفاعل القانوني معه يقف عند حد معين لم يتجاوزه، وفي هذا ما يجعل مناطق الخلاف قائمة بين هذا الدليل وبين الدليل في صورته التقليدية، وكذلك ما يسمى بالدليل العلمي الذي يجد أساسه في منطق وقواعد فرع من فروع العلم كالطب والهندسة ... الخ.

وإذا كنا فيما سلف قد انتهينا الى إمكانية الاستعانة بالدليل المادي الذي يستخدم فيه أدلة الإثبات المقررة والمعروفة في القانون للحصول على ما يفيد الإدانة او ما يثبت حقوق العدالة عموما، سواء حق المجتمع في الإدانة او حقه أيضا في ثبوت براءة الشخص، وهو أمر اتبعه القانون الهولندي حين القبض على الشاب الهولندي الذي ابتكر فيروس Anna Kornicova بمجرد قيامه - بتوجيه من والديه!! بتسليم نفسه الى السلطات الهولندية، فإن الاستعانة بالدليل الرقمي تجعل موضوع مثل هذه النقطة محلا لكثير من الشك في قيمته كدليل يتواءم مع مفهوم الأدلة التي يعرفها القانون في صيغته التقليدية.

وفي هذا الفصل سوف نتولى استجلاء الدليل الرقمي فنحدد تعريفه (مبحث أول) وخصائصه (مبحث ثان)، وأنواعه (مبحث ثالث).

المبحث الأول
التعريف

يتجه بعض الفقه المقارن الى التوسع في تعريف الدليل التقني او الرقمي Digital Evidence او الالكتروني Electronic Evidence فهو **"كل بيانات يمكن إعدادها او تخزينها أو تراسلها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما"**.

على أن ربط الدليل الرقمي بفكرة المعلومة يجعل موضوع الدليل الرقمي يؤدي دوره في إطار عملية استرجاع او استرداد المعلومات فقط، وبحيث لا يكون دليلا سوى كل ما يمكن استرجاعه او استرداده من معلومات. حين أن منطق التعامل مع الحاسوب يمكن أن يكون أساسه التعامل مع بيانات متكاملة قد يكون من المعتاد ظهورها على شاشة الحاسوب لكي يمكن التعرف عليها، ولكن لا يعد ذلك شرطاً يلزم وجوده.

لذلك - وعندنا - يمكن تعريف الدليل الرقمي بأنه **"الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة"**. فهو ذلك الجزء المؤسس على الاستعانة بالمعالجة التقنية للمعلومات، والذي يؤدي الى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الانترنت. فكلما كان هناك مزج في موضوع الدليل (الفكرة او المعلومة كبيانات Data.. الخ) بالمعالجة الآلية للمعلومات فإنه يعد هنا دليلا رقميا[2].

والدليل الرقمي تشير مقدمات التعامل معه بكونه يعبر عن تجاوب متكامل يتطور بسرعة كبيرة جدا، فبعد أن كان الدليل الصامت يشير الى ما يمكن الحصول على نسخة منه بطريق الطباعة Print – out، وهو ما يسمى بمخرجات الحاسوب مثل الوثائق Document والصور Pics.. الخ، فإن التطور اقتضى أن يكون له منطق أخر الآن يُعبّر عنه التطور ذاته الذي تنتجه تقنية المعلومات، وهو المظهر التقني المعلوماتي المتسم بالحركية والذكاء.

ومن ثم فإن موضوع أمكان اعتبار الدليل الرقمي بالمفهوم التقليدي– بطريق الطباعة، واعتبار هذه المخرجات أدلة تأخذ بها المحاكم في القانون المقارن، يبدو إنه قد أضحى تاريخا إذا علمنا إن التطور قد فرض نوعية اخرى ذكية وحركية تندرج في الدليل الرقمي وتُعد أحد أشكاله الجديدة، مثلما هو الحال في نوعية الملفات التي تحتوي في موضوعها ما هو غير معد للطباعة، كتلك التي يتم إعدادها في الحاسوب للقيام بالربط بين الحواسيب، وكذلك تلك التي تتولى الربط بين الخوادم عبر الشبكات الخاصة. فاليوم لم يعد الامر مرتبطا بفكرة الحاسوب الشخصي PC بل تطورت التقنية لتضع لنا، فضلا عن تطوير الحاسوب الشخصي ذاته PC، بإضافة إمكانيات ضخمة إليه، نظم الشبكات Networks والمعالج التوزيعي Distributed processing ثم أخيرا الانترنت[3].

ولعل النقاط التي يمكن أن تثار في إطار الدليل الرقمي يمكن أن تظل محل استفهام لدى فكر الإثبات التقليدي، فالحصول على الدليل في منطق الفقه التقليدي سوف يختلف حاله عن النهج في الدليل الرقمي،

---

[2] **Amanda Hoey - Analysis of the police and criminal evidence act sec. 69 / computer generated evidence - WEB Journal of Current Legal Issues UK, 1996 Issue 1, p.1 . Available online in june 2000 at Http://webjcli.ncl.ac.uk/1996/issue1/hoey.html**

[3] **Peter Sommer – Digital footprints: assessing computer evidence, Criminal law review, special edition 1998 , Uni . of Man. UK . P. 65**

الذي ليس بلازم أن يتم الحصـــول عليه في مكان الحادث، وإنما من الممكن أن يتم الحصـــول عليه حيث الملقمات servers ، وهو أسلوب IP Crack، إذ يسمح الطرف الثالث، بشروط يتطلبها القانون، بتزويد أي كان بمعلومات عن المتصفح الذي يلج الى صفحات الغير، فيتم تعقبه عبر الخادم والمضيف، ومن ثم فإذا عرف المضيف أمكن الاتصال به والسؤال عن عنوان الانترنت IP - Internet address الخاص بأي كان والذي قام بتصفح الصفحة الخاصة بالمجني عليه، وهو الأمر الذي يمكن أن يكون عرضة لتساؤل بحثي على درجة من الخطورة، سيما إذا علمنا إن هذه أحدى الوسائل التي يلجأ اليها عادة، فهل يسمح القانون للغير بتعقب المتصفح حين دخوله على صفحة او صفحات ما؟ خاصة إذا علمنا أن الفحص هنا قد يتم عبر الحدود الإقليمية في العالم المادي بحيث يتجاوزها الى داخل حدود دولة او مجموعة دول أخرى.

بالإضافة الى أن الأمر قد يشتبه فيه عدوان على الحرية الشخصية حال علمنا إن الامر يخرج عن طائلة الجريمة، وإنما يخضع لمبدأ المراقبة فقط CyberSevillance دون أن يكون هناك جريمة ما. وهذا الأمر الأخير يقود الى سؤال يتمثل في أن الافتراض الذي قد تقود مقوماته سلطات منع الجريمة ربما يجعل الأمر سهلا في تعقب الجريمة والمجرمين من خلال تطويع التقنية لكي تعمل في بيئة الرقابة، وهو أمر لا يزال التشريع التقليدي يرفضه بضراوة، حتى في ظل الضمانات الإجرائية التي لا تشكل موضوعا بقدر ما ينظر اليها كاستثناء على الأصل وهو المنع (انظر مثلا المواد 206 - ا. ج مصري – 309 مكرر عقوبات مصري). ولازالت مسألة مراقبة الحركة عبر الانترنت من الموضوعات الخطرة، ففي قضية Scarfo قامت المباحث الفيدرالية FBI بطلب أذن بمراقبة حاسوب المدعو Scarfo لكونه يتعامل بالانترنت بشكل إجرامي، وحين تقدمت بطلب اذن لكي تجري هذه المراقبة على حاسوب المدعو Scarfo رفض القاضي الدليل المستمد من هذه المراقبة لكونها تمت بشكل ينم عن عدوان على الحياة الخاصة.

المبحث الثاني
خصائص الدليل الرقمي

إن التعامل مع الدليل الرقمي يُعد بالضرورة من متطلبات التعامل مع الانترنت والحاسوب وتقنياته من قطع صلبة وبرمجيات، لذلك فإن الإلمام بكل هذه الأمور قد يكون من الأمور الطبيعية هنا. وقولنا الإلمام لا يعني لزوم أن يكون هذا الإلمام له مقومات شكلية معينة تستلزم دراسات أكاديمية، وإنما تحتاج الى الخبرة فيها الى فهم تقني لها، وجدارة في التعامل مع الخيال العلمي الرقمي الذي أنتجته ثورة المعلومات. لذلك فإن أول خصائص الدليل الرقمي اتصاله بتقنية تكنولوجيا المعلومات/ الانترنت بإعتباره البيئة التي يتواجد فيها.

فإذا تأملنا موضوع الدليل الرقمي فإنه، بدون شك، لن يكون له تلك الطبيعة التي عليها الأدلة التي يمكن تحقيقها في العالم المادي، لكونه قابع في العالم الافتراضي المبني على الكيفية المعنوية غير الملموسة Intangible، وهذا الأمر يشكل قالب الدليل الرقمي في تكنولوجيا المعلومات/ الانترنت وبالتالي يعد الخصيصة الثانية له.

هذا الطابع المعنوي الذي عليه الدليل الرقمي من طبيعة أصلية، ومسألة الاصالة هذه أثارت العديد من المشكلات من حيث مدى الاعتداد بالنسخة التي تشكل دليلا كاملا هنا، حتى إنه برز الأمر في اطار حصره في عامل الثقة التي يجب أن تتوافر فيمن يحصل هذا الدليل، وبين من يقوم بالتعامل معه أيضا. وتلك هي الخصيصة الثالثة التي يجب أن تؤخذ في الاعتبار. أيضا الدليل الرقمي من الأدلة التي يصعب التخلص منها، وهذه الخصيصة الرابعة التي تجعل هذا الدليل له طبيعة مختلفة تماما عن الأدلة المادية.

وفيما يلي نطرح لخصـائص الدليل الرقمي المذكورة بشـيء من التفصـيل يفيد في اسـتجلاء حقيقته وعلى النحو الذي يحقق إمكانية التعامل القانوني معه، وهو الأمر الذي يسـاعد على محاولة فصـله عن الدليل المادي:

أولا: الدليل الرقمي دليل علمي: - الدليل الرقمي يحتاج الى مجال تقني يتعامل معه، فهو دليل يحتاج الى قدر من التجاوب مع البيئة التقنية، وهذا يعني إنه كدليل يحتاج الي بيئته التقنية التي يتكون فيها لكونه من طبيعة تقنية المعلومات. ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي. فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة **(إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة** Law seeks justice ; Science seeks truth)، حتى على الرغم من الانتقادات التي توجه الى هذه القاعدة من حيث الالتزام الذي يلقيه القانون والقضاء المقارن على عاتق أعضائه بضرورة توافر **معرفة علمية** Scientific knowledge **لكي** يمكن إقامة بنيان التمييز بين ما هو قانوني وبين ما هو علمي[4]. وهذه مسألة شاقة لكون القضاء يحتاج الى الخبرة القضائية في شأنها، وهو أمر جعل بعض القضاء يتجه الى الاكتفاء بالخبرة لكي تكون مرتكزة في هذا الشأن وهو رأي مردود من حيث أنه جعل القضاء مجرد ناقل لرأي الخبير دون أن يعرف محتوى الخبرة وموضوعها.

وإذا كان الدليل العلمي له منطقه الذي يجب ألا يخرج عليه من حيث لزوم عدم تعارضه مع القواعد العلمية السليمة، فإن الدليل الرقمي له ذات الطبيعة، إذ يجب ألا يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه.

وعدم الخروج عن متطلبات العلم الرقمي لا يعني أن هناك قواعد جامدة يرتبط بها الدليل الرقمي من حيث طبيعته العلمية، وإنما يجب الأخذ في الاعتبار إن العلم الرقمي هو علم متطور جدا، بل إنه يجد ذاته في قدرته الكبيرة على التطور الذاتي المستمر، سيما من حيث كونه لا يستجيب للقاعدة التقليدية المدرسية، حيث إنه يمكن ان يكون هناك خبراء في العالم الرقمي لم يتم أي منهم منهج دراساته التقليدي المتبع في التدريس، ولا يملك الشهادات والدرجات العلمية أيضا ومع ذلك برعوا في العلم الرقمي وأصبح كل منهم خبيرا فيه.

ثانيا: الدليل الرقمي من طبيعة تقنية: - وكنا فيما سلف قد طرحنا موضوع التقنية ومحاولة تعريفها، وهنا نتعرض الى التقنية من حيث كونها مصدرا للدليل الرقمي، وهذا يستدعي في الحقيقة مناقشة دورها في تكوين هذا الدليل الذي يصلح كما هو مذهب، او محاولات تمذهب، القانون المقارن على الاعتداد به لتكوين قاعدة الإدانة والبراءة.

فالدليل الرقمي ليس مثل الدليل العادي، فلا تنتج التقنية سكينا يتم به اكتشاف القاتل او اعترافا مكتوبا او مالا في جريمة الرشوة او بصمة إصبع ... الخ. وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها. ومثل هذا الأمر لاحظه المشرّع البلجيكي فقام، بمقتضى قانون 28 نوفمبر 2000 بتعديل قانون التحقيق الجنائي Code

[4] **The search for scientific knowledge in federal courts in the post- fryer era : refuting the assertain that law seeks justice while science seeks truth - howard a. denemark - Berkeley techology law journal vol. 8 / 2 , p. 15 . available online in jan 2001 at**
http://www.law.berkeley.edu/journals/btlj/articles/08_2/Denemark/html/text.html

d'instruction Criminelle بإضافة المادة (39 bis) التي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية.
وإذا كانت الانترنت محلا لما هو مشروع فإنها كذلك قد تكون وسيلة لارتكاب جرائم وأعمال غير مشروعة، فقد أمكن تشكيل منظمات عصابية عبر الانترنت دون أن يكون هناك تواصل مادي بين اشخاص المجرمين، وكذلك القيام بجرائم عبر الانترنت كالنصب والاحتيال والدخول على المصارف وإجراء تحويلات غير مشروعة...الخ، وببساطة فإنه عبر الانترنت يمكن أن يرتكب أي شخص جريمة في الوقت الذي يقوم فيه بالتبرع بالمبالغ المحصلة من الجريمة الى احدى الجمعيات الخيرية.

ومن ثم فإن إطلاق الصفة الرقمية إنما تعني إنه ينبغي أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها[5]، سواء كانت الجريمة المرتكبة احتيالا على بنوك او مؤسسات مالية، او كانت الجريمة قذفا وسبا او تشهيرا علنيا في حلقات النقاش او القوائم التراسلية او غيرها وكذلك بثا وتداولا لصور وأفلام دعارة أطفال. ومثل هذا الأمر يجعلنا نقرر إنه لا وجود للدليل الرقمي خارج بيئته التقنية او الرقمية، وإنما يجب لكي يكون هناك دليل رقمي أن يكون مستوحى او مستنبطا او حتى مستجلب من بيئته التي يعيش فيها وهى البيئة الرقمية او التقنية، وهي في إطار جرائم الانترنت ممثلة في العالم الرقمي الذي يطلق عليه العالم الافتراضي، وهو العالم الكامن في الحاسوب والخوادم والمضيفات والشبكات ويتم تداول الحركة فيه عبرها.

ثالثا: الدليل الرقمي مفهوم يحتوي التنوع والتطور: - إن مصطلح الدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، وبحيث يكون بينها وبين الجريمة رابط من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذا الرابط بينها وبين الجاني[6].

وإذا كانت العلاقة أساسية بين البيانات الرقمية وبين الدليل الرقمي، لكون الأخير إنما هو القالب الذي يحتوي في داخله مجموعة البيانات الرقمية، فإن ذلك يعد تعبيرا عن اتساع قاعدة الدليل الرقمي، وبحيث يمكنه أن يشمل أنواعا متعددة من البيانات الرقمية تصلح منفردة او مجتمعة لكي تكون دليلا للإدانة او للبراءة. إذ يشمل هذا التنوع في البيانات الرقمية مظاهر عدة، كأن يكون هذا المحتوى معلومات متنوعة تتضمن نصوصا وصور وسمعيات ومرئيات.

ولما كانت البيئة التي يعيش فيها الدليل الرقمي بيئة متطورة بطبيعتها، وإن تطورها، الذي يكاد يكون تلقائيا هنا، يتسع لإمكانية شمول مظاهر رقمية جديدة، سيما وإن المبدأ في العالم الافتراضي إنه لا يزال في بداياته ولم يصل بعد الى منتهاه. فالعالم الرقمي لا ينتهي ولن يكون من السهولة احتوائه، فهو عالم متسع لأبعد مما قد ينتجه الخيال من أفكار حول الحدود. وهذا إشارة واضحة الى كل من يكون مسعاه التوصل الى سيطرة من أية نوع على العالم الافتراضي، فإذا استطاع شخص او دولة مثلا التوصل الى إمكانية وضع حدود رقابية على هذا العالم فإن ذلك لا يعني عدم إمكانية قيام شخص او دولة اخرى بإعداد حدود تعارض هذه الرقابة، وبشكل يعطل أية رقابة على الإطلاق دون أن يكون هناك لزوم للحصول على أذن مسبق في هذا الشأن.

---

[5] **Amanda Hoey - Analysis of the police and criminal evidence act sec. 69 / computer generated evidence - web journal of current legal issues UK , 1996 issue 1, P. 2**

[6] **Eoghan Casey - Digital evidence and forensic science , computer and the internet , computer crime - 1st ed. academic press - USA UK 2000 . P. 9**

رابعا: الدليل الرقمي يصعب التخلص منه: - وهذه إحدى أهم خصائص الدليل الرقمي على الإطلاق، بل إنه يمكن عداد هذه الخصيصة ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة الأخرى، بحيث يجب هنا إحداث مقارنة بين الدليل الرقمي وبين الدليل الجيني Genetic form of evidence، او ما يطلق عليه DNA وبالعربية الحمض النووي. وذلك لاتحاد كليهما في هذه الخصيصة، وهي صعوبة التخلص منهما من ناحية، ومن ناحية أخرى يمكن إحداث تعديل في تكوينهما معا. وهذا يعني إن مقارنة بين الدليل الرقمي وغيره من الأدلة التقليدية في هذه الناحية من الأمور التي يكون فيها التجاوز واضحا، وبحيث يدل ذلك على انعدام وجود أساس صحيح لبناء هذه المقارنة.

أن الأدلة التقليدية التي يعرفها القانون تجد قوتها أمام القضاء في مسألة التسريع بالحصول عليها، فبصمات الأصابع مثلا يمكن أن تكون محل شك إذا طالت المدة بين ساعة ارتكاب الجريمة وبين الحصول عليها.

كذلك الشهادة إذا مضى عليها مدة طويلة من الزمن فإن مسألة الاستعانة بها تخضع لتحقيق متواصل بحيث يجب التعرف على مدى قدرة الشاهد على التذكر والعوامل المؤثرة في الذاكرة وما إذا كان يتمتع بمستوى ذاكرة مقبول في مستوى الرجل العادي الذي يعرفه القانون .... وفوق ذلك كله فإن مسألة التخلص من الأدلة المادية تظل من الموضوعات التي يأخذها القانون في الاعتبار ويرتب عليها آثارا ما، إذ يمكن التخلص من بصمات الأصابع بمسحها من موضعها، كما إنه في بعض الدول الغربية يتم التخلص من الشهود بقتلهم او تهديدهم بعدم الإدلاء بالشهادة حتى إن دولا مثل الولايات المتحدة الامريكية - نتيجة لاستفحال الجريمة فيها بشكل تهديدي خطير - ابتكرت برنامجا لحماية الشهود يتم فيه تغيير الحالة المدنية للشاهد مطلقا بحيث يكتسب شخصية وكينونة جديدة مع توفير بيئة جديدة له، حتى لا يتم التعرف عليه والانتقام منه من قبل المجرمين الذين تمت أدانتهم بسبب شهادته. وكذلك يمكن التخلص من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرارات بارتكاب شخص او أشخاص لجرائم وذلك بتمزيقها وحرقها... الخ. وكل ذلك بالطبع يجعل عملية التخلص من هذه الأدلة المادية أمرا سهلا، حيث إنها جميعها لن يكون من السهولة- بل ومن الاستحالة بمكان- استرجاعها او استرداد الدليل المستمد منها حيث انها تم تدميرها كلية.

وإذا كان الأمر كذلك بالنسبة للأدلة التقليدية فإن الحال غير ذلك بالنسبة للأدلة الرقمية، ذلك إن موضوع التخلص من Discard الدليل الرقمي باستخدام خصائص التخلص من الملفات في الحاسوب او الانترنت كخاصية Delete وRemove وErase.. الخ، لا تعد من العوائق التي تحيل دون استرجاع الملفات المذكورة، إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها او أزالتها من الحاسوب[7].

ولقد كانت قضية إيران - كونترا Iran - Contra من أولى القضايا التي أبرزت الطبيعة التي عليها الدليل الرقمي وما يتمتع به من صلابة، ففي هذه القضية أدرك المسئولون في الحكومة الامريكية (مستشار الأمن القومي)[8] عدم وجود اتزان في مقارنة الدليل الورقي بالدليل الرقمي، فالدليل الورقي يمكن التخلص منه بتمزيق الورقة التي تحمله في حين إن الدليل الرقمي يمكن أعادته الى الحياة، حتى وإن كان قد تعرض للإزالة. ولقد ترتب على هذا الأمر أن قامت الإدارة الأمريكية بالاطلاع على نظام الحفظ Backup للبريد الالكتروني فتبين تورط بعض المسئولين في مكتب الرئيس الأمريكي[9]. ويترتب على هذه الخصيصة مسائل

---

[7] وذلك من منطلق الثقة في تكنولوجيا المعلومات حيث ان التقنية يمكنها القيام بتحقيق الخيال الإنساني دون حدود .

[8] The National Security Adviser – John Poindexter

[9] Christine Sgarlata Chung & David J. Byer - The Electronic Paper Trail, op -cit at 6.

هامة في القانون، أبرزها على الإطلاق مسألة التخلص من الدليل، وهو الموضوع المعاقب عليه بمقتضى القانون، فمثلا إن إعداد برمجيات يتم التعويل عليها من قبل مرتكبي جرائم الحاسوب عامة والانترنت تخصيصا مهمتها هي التخلص من الأدلة بإزالة محتويات الحاسوب والبرمجيات التي يستخدمها هؤلاء في ارتكاب جرائمهم من الأمور غير المفيدة، حتى ولو تضمنت إمكانية التخلص من الأدلة في جريمة معينة، فاذا أثبت الخبير التقني مثلا ان مرتكب الجريمة استخدم مثل هذه البرمجيات للتخلص من الأدلة فإنه يمكن إدانة مرتكب الجريمة بالنصوص التي تجرّم مثل هذه الأفعال، سيما وان ما توصل إليه الخبر يثبت حدوث هذه الجريمة، وعندنا إن المشرّع الجنائي مطالب في هذه الناحية بتقوية عناصر النصوص القانونية التي تجرّم التخلص من الأدلة بتخصيص منطق رقمي فيها يجعل التشديد وجودا فيها حال وجود علاقة بين التخلص من الأدلة وبين العالم الرقمي.

المبحث الثالث
أنواع الدليل الرقمي

ليس للدليل الرقمي هيئة واحدة، وإنما له خصيصة الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، إذ يتكون من الطابع الثنائي وهو (1 - 0) بالطبع، وأما تكوين بياناته فإنها تختلف من حيث الحجم والموضوع. إذ إن كمية الـ.. (1 - 0) في ملف ما يمكن أن تختلف عن الحجم في ملفات أخرى.

ومثل هذا الأمر ليس له تأثير سوى من حيث تكوين الملفات، على إن الحجم هنا يمكن أن يكون محل دفع أمام القضاء لمعرفة الملف الأصل حين المطالبة بعقد مقارنة بين الملفات لمعرفة حجم الخسائر التي تعرض لها الموضوع الفيزيقي للحاسوب، أي محتوياته، او الخادم او الملقم او حتى الشبكة ككل.

ومقصود التنوع في الدليل الرقمي يفيد بالضرورة انه ليس هناك وسيلة واحدة للحصول عليه، وانما تتعدد وسائل التوصل اليه، في كل الأحوال يظل الدليل المستمد منه رقميا. حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسسا على طابع افتراضي مبناه أهمية الدليل الرقمي ذاته وضرورته إلا إنه لكي يحدث تواصل بين القانون وبين الدليل المذكور[10] فإنه يلزم سلوك مسلك الافتراض من حيث اعتباره دليلا أصليا.
ويعود سبب التنوع في مصادر الحصول على الدليل الرقمي الى كون الانترنت تكتسب وجودها وحياتها من ضرورة توافر مقدمات متعددة لها، كالحاسوب والشبكات والمعلومات التي تتراسل، وكذلك المحتوى المادي للمعلومات كبرمجيات التعامل مع المعلومات في العالم الافتراضي وكذلك التطبيقات.. الخ، وهذه كلها تعد من مصادر الأدلة إذا تم فحصها لكونها تشكل قواعد اختراق. وإن كان يؤخذ في الاعتبار الحيز المادي الذي توضع فيه الآليات التي تعمل على توصيلنا بالانترنت، وقد يستقى منها دليل او آخر يساعد في كشف غموض الواقعة او وقائع أخرى قد تكون في ذاتها جرائم أخرى او ارتباط بالجريمة موضوع البحث[11].

فمثل هذا الحيز المادي كنا قد تعرضنا له حال تطرقنا الى بحث الدليل في صورته التقليدية، حيث تطرقنا الى التفتيش فيما سلف، وهو يشمل التطرق الى فحص الحيز المكاني الذي توجد فيه الأداة الحاسوبية التي

---

[10] نتيجة لنقص توافر الإمكانيات الرقمية في المحاكم.

[11] Testimony of Kevin R. Mitnick / u.s. senate governmental affairs committee, op - cit

توصلنا بالانترنت، كما هو الشأن في تفتيش المكاتب والغرف والأدراج والأوراق والسجلات والحقائب وغيرها قصد الحصول على ما يفيد في كشف الحقيقة.

ومثل هذا الإجراء ينبغي عدم التنازل عنه لمجرد إن موضوع الجريمة يتعلق بحاسوب او انترنت، حيث إنه من الممكن أن يكون مرتكب الجريمة أكثر حذرا مما تتصور سلطات التحقيق او الاستدلال، فيقوم بنسخ او طباعة Printout محتوى جريمته الحاسوبية، وهو أمر ليس بعيد الاحتمال إذا تأملنا الفكرة من زاوية النصائح التي يتقدم بها صناع برمجيات الحاسوب من ضرورة إعداد نسخة مكررة احتياطية Backup من برمجيات الحاسوب العامل لمواجهة الظروف الطارئة.

وفي هذا المطلب سوف نعالج كيفية الحصول على الدليل الرقمي، حيث يتطلب ذلك فحص نظام الاتصال بالانترنت (مطلب أول) ثم نتطرق الى فحص مركبات الحاسوب (مطلب ثان).

مطلب الأول
فحص نظام الاتصال بالانترنت

يُقصد بنظام الاتصال بالانترنت بالمفهوم الاجرائي مدى إمكانية اقتناع محكمة الموضوع بالإجراءات المتبعة حال استخدام وسيلة الاتصال بالانترنت. ومن ثم يستلزم الحال هنا التطرق الى الإجابة على السؤال المنطقي في إطار الاجراءات الجنائية وهو كيف حدثت الجريمة؟ مع لزوم أن تكون هذه الإجابة منطقية متوافقة مع ما هو مقرر في القاعدة الإجرائية.

وفي هذا الإطار تثار مسائل شتى، ذلك إن الانترنت من طبيعة مرنة فلا يوجد لها مالك كما إنه ليس هناك من يمكنه التسلط عليها، وهو الامر الذي جعل تراجع خاصية التتبع في الاجراءات الجنائية أمرا واقعا او بالكاد. ولعل أهم المسائل المثارة في صدد فحص نظام الاتصال بالانترنت، سعيا وراء إقامة الدليل على الإدانة، هي مسألة مدى إمكانية تحديد مكان الجريمة او الحاسوب الذي أنطلق منه النشاط المادي للجريمة، ومثل هذا الامر وإن كان لا يقود تحديدا الى الشخص مرتكب الجريمة استنادا الى الدليل الرقمي فقط الا انه يمكن ان يساعد حتما في التوصل اليه عبر إقامة الدليل التقليدي فيما بعد. على إن الامر لا يقف عند هذا الحد، وانما يمتد الى ضرورة التطرق الى تقصي الحقيقة في أماكن اخرى مثلما هو الحال في فحص كل ما يتعلق بنظام الاتصال بالإنترنت، كالشبكات المحلية والعالمية والبيانات وحركة الاسترداد والنظام الأمني المحاط بالإنترنت ونظام الاتصالات القائم وحركته وإمداداته وبرمجيات الانترنت وحركة الإنزال والتحميل والنظام المعلوماتي المحمل على الانترنت ودرجة استيعابه ... الخ. هذه كلها يلزم فحصها توصلا الى دليل رقمي يفيد في كشف الحقيقة، فلا يقف الامر عند مجرد ابراز العجز عن التقصي والبحث والتفتيش هنا، فقد يمكن من خلال استطلاع أي من هذه الوسائل القيام برصد دليل رقمي ما.

ذلك أن الدليل الرقمي على الرغم من اتساع قاعدته إلا إنه يمكن أن يكون متواجدا في صيغة ما لا يمكن توقعها، فمثلا نجد أن التفتيش والتقصي في الحاسوب الشخصي سعيا وراء البحث عن ملف ما ، يرتبط بارتكاب جريمة موضوع هذا التقصي والبحث من قبل الخبير، قد لا يؤدي الى نتيجة ما تذكر ، إلا إن البحث في نظام البريد الالكتروني قد يؤدي الى وجود ما يفيد في إثبات الجريمة، كما لو كان مرتكب الجريمة قد قام بوضع نسخة من هذا الملف في خادم البريد الإلكتروني/عبر الانترنت والخاص بهذا الشخص بحيث يمكنه أن يطاله من أي مكان وفي أي وقت.

لذلك نتناول فيما فحص نظام الاتصال بالانترنت في محاولة لتقسيم هذا النظام بحسب المناطق التي يتكون منها، وهذا نظام تقسيم مادي مستمد من تفصيل الانترنت التقني، وهو تفصيل- على أية حال- لا يرتبط بضرورة تسلسله، وإنما يمكن القيام باتخاذ هذا او ذاك الإجراء دون أن يكون مرتبطا بهذا التسلسل.

أولا: مسار الانترنت: - تعني عبارة **مسار الانترنت** Routing الحركة التراسلية للنشاط الممارس من خلال الانترنت، فالحاسوب بمجرد أن يتعرف على المسار يقوم تلقائيا باختيار البروتوكول التراسلي Le protocole de transmission الذي من خلاله يقوم باستدعاء البيانات[12]، وهى الحركة التي أشار إليها علماء الانترنت على إنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها، لذلك يطلق عليها الشبكة العنكبوتية.

ويُستخدم في تتبع حركة مسار الانترنت نظام الفحص الإلكتروني Electronic Trail الذي يُطلق عليه علم البصمات المعاصر او علم بصمات القرن الواحد والعشرين "Electronic trail" is the fingerprint of the twenty-first century[13]، وهو منهج متبع في تتبع الحركة العكسية لمسار الانترنت، ولقد تم تطبيقه على أكثر من جريمة، مثل تتبع مبتكر فيروس ميليسا Melissa virus وكذلك في التوصل الى الشخص الذي ابتكر موقع خدمات بلومبرج لأخبار المال الإحتيالي لكي يرفع أسعار الأسهم بطريق الخداع.. الخ[14].

ويتنازع إمكانية تحديد مسار الانترنت من عدمه رأيان ، فيذهب رأي الى إنه لا يمكن تحديد مسار ارتكاب الجريمة [15] ، وتكمن وجاهة هذا الرأي في إن الانترنت مرنة الطبيعة بحيث أنه حتى وإن أمكن مستقبلا تحديد مسار الانترنت فإن ما يتم الحصول عليه في هذا الإطار إنما هو دليل رقمي يحتاج الى تكملته بأدلة إثبات اخرى ، فيما لو اقتصر الامر على هذا الدليل فإن الامر يظل في حومة الشك ، ذلك إن ما يتم التوصل اليه في الحقيقة من خلال الدليل الرقمي إنما هو عنوان رقمي فقط IP address وهو لا يكفي في نسبة العمل الإجرامي او غير المشروع الى صاحب او مالك الحاسوب او عنوان الاسم المذكور، إذ من الممكن ألا يكون هو مرتكب الجريمة حقا ، كما لو كان حاسوبه مسروقا او مؤجرا (في مقهى انترنت) او أن يكون عنوانه الرقمي مسروقا او مختلسا او أن يكون أحد يستخدمه احتيالا ، وكذلك لن يكون له أي تأثير في الإدانة إذا تبين إن المتهم لا يعرف عن الانترنت او حتى الحاسوب أي شيء . فمثل هذه الأمور تجعل من الصعوبة بمكان إمكانية الاعتماد على مسار حركة الانترنت للتوصل الى المتهم، وإنما يحتاج الامر هنا الى دليل مادي ومثابرة من جهات الاستدلال والتحقيق لكي يتوافر لها دليل مادي كاعتراف او شهادة او خبرة او قرائن.. الخ. بل إنه حتى في إطار الأدلة المادية ينبغي ألا تتجاوز الى تقرير المستحيل وبما لا يتفق وطبيعة الانترنت، وعلى محكمة الموضوع عدم الخروج على الطبيعة التي عليها تقنية الانترنت وبما يتجاوزها فتقرر أحكاما لا تتفق ما طبيعة الأشياء، بل يجب أن يكون القاضي مدركا لها ومحيطا بطبيعتها

---

[12] Vincent Grynbaum - Le droit de reproduction à l'heure de la société de l'information , A propos de la Directive 2001/29/CE du parlement européen et du conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information , op cit P. 2

[13] FOURTH AMENDMENT AND THE INTERNET, Hearing Before The Subcommittee on the constitution of the committee on the judiciary house of representatives one hundred sixth congress second session april 6 2000 serial no. 135, op – cit.

[14] FOURTH AMENDMENT AND THE INTERNET, op cit "The creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California" .

[15] د . جميل عبد الباقي الصغير – الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – المرجع السابق ص . 44

وعالما بحركتها وإمكانياتها الهائلة. ويمكن التأكيد على إنه حتى في الحالات التي تمت فيها إدانة أشـــخاص أمام القضاء المقارن كان هناك دائما دليل مادي يتم الاستناد اليه الى جوار الدليل الرقمي في هذا الشأن.

في حين يذهب رأي آخر تزعمته محكمة باريس في حكم حديث لها[16] الى إمكانية تتبع مســـار الانترنت، وبالتالي يمكن التوصـــل من خلال هذا التتبع الى تحديد مســـار العمل الاجرامي. ولقد قامت محكمة باريس الابتدائية بتبني هذا الرأي بناء على اعتماد تقرير خبرة في هذا الإطار، ويبدو إنه من الأهمية بمكان أن نعرض لرأي محكمة باريس بشـــيء من التفصـــيل لكي يمكن التعرف على هذا الرأي وبالتالي تحديد مدى جدارته هنا:

ـ أســانيد الرأي القائل بامكانية تحديد مســار الانترنت (قضــية ياهوو) :- بدأت وقائع هذه القضــية عندما فوجئ أنصـــار الصـــهيونية بوجود مزاد علني Auction على أحدى الصـــفحات المجانية التي تبث من خلال موقع Yahoo! على الانترنت www.yahoo.com، ولقد تضـمن هذا المزاد مجموعات من صـور لزعيم المانيا النازي أدولف هتلر ، وكذلك أعلام النازية وشـــعاراتها ومجموعة صـــور مختلفة وصـــل مجموعها الى (1179) بند ، كلها تتضـــمن إشـــارة او أخرى الى فترة العصـــر النازي في المانيا. ومن ثم تحركت القوى التقليدية المضـــادة للنازية لمناهضـــة هذا الموقع. ولما كان البث عبر الانترنت يأخذ الطابع العالمي الذي يعترف بالحدود فقد تم اختيار فرنسا لكي تكون محطة التقاضـي في هذا الإطار سيما وإن بها قانونا يتعلق بمكافحة النازية.

ولقد تولى القضية في فرنسا اتحاد الطلبة اليهود في فرنسا[17]، والمنظمة الدولية لمكافحة العنصرية وأعداء الصهيونية (ليكرا)[18]. حيث أقيمت الدعوى في شهر أبريل 2000 في محكمة باريس الابتدائية، على أساس قيام ياهوو بالتقليل من موضوع كارثة الهولوكوست "Banalizing the Holocaus "، مما يعني إفساح المجال للعامة في هذا المجال، وهو الامر المجرم في القانون الفرنســـي وذلك بالســـماح بوجود مزاد علني عبر موقع Yahoo من خلال الصـــفحات المجانية فتضـــمن المزاد المذكور نماذج من الزمن النازي تبث يوميا عبر الانترنت كأفلام وملصقات وملابس خناجر Daggers وصور ورسوميات وميداليات وشعارات ... الخ.

ولقد رفعت القضـــية إمام القاضـــي Jean -Jacques Gomez في محكمة باريس. ولقد حاولت شـــركة Yahoo! الدفع بعدم الاختصـــاص لكون القضـــاء المختص هو القضـــاء الامريكي، ولكون الشـــركة شـــركة أمريكية ومسـجلة في أمريكا، وهو أمر إن قبل أمام القضـــاء الفرنســـي لترتب عليه فشـل الدعوى القضـــائية، لكون القانون الأمريكي يســـمح بقدر من الحرية وفقا للتعديل الأول من الدســـتور الامريكي، إلا أن القضـــاء الفرنســـي رفض هذا الدفع مقررا اختصـــاصـــه في هذا الإطار. وفي 15 مايو 2000 قام اتحاد الطلبة اليهود في فرنسا بمد خصومته الى Yahoo! فرنسا حتى يكون الاختصاص منعقدا للقضاء الفرنسي تماما وبالتالي يغلق الباب أمام Yahoo! العالمية في إطار موضوع الاختصاص هذا.

ولقد انحصـــرت طلبات المدعي هنا على أن تقوم Yahoo فرنســـا بإزالة كل خطوط نشـــطة مرتبطة Hypertext links بـ ... Yahoo Inc.، التي سمحت ملقماتها بوجود مواد ذات طابع عنصري Racist material، ثم ذهب المدعي الى أبعد من ذلك عندما طالب المدعي عليه صـراحة بتحذير ملقمات الانترنت

---

16 **UEIF & Licra c. Yahoo fr. / Yahoo inc. TGI Paris, decision du 22 Mai 2000.**

17 **The Union of French Jewish Students (UEJF)**

18 **The International League Against Racism & Anti-Semitism (LICRA)**

الفرنسية من مثل هذه المواد العنصرية الموجودة في Yahoo العالمية، ومن ثم فإن الإبحار او التصفح من خلال Yahoo العالمية ذات الأساس الأمريكي يمكن أن يكون مدعاة الى وجود اختراق للقانون الفرنسي.

وفضلا عن كون **Yahoo** طعنت في اختصاص القضاء الفرنسي، فإنها أيضا جادلت في انتفاء نية تعظيم النازية او دعم المعتقدات التي تدعو الى ذلك بطريق الربط على **Yahoo Inc.**، بل وأبعد من ذلك فقد أكدت **Yahoo** فرنسا إنها لا تقدم دعم الدخول **Access** للمواقع التي تتضمن موضوعات غير مشروعة عبرها، وهو ما تتضمنه وثائق **Yahoo** عبر الانترنت التي تشير الى ضرورة احترام مبدأ عدم الإساءة لكافة المشتركين فيها ومستخدمي ياهوو والمستفيدين من خدماتها عبر الانترنت. ولقد أصدر القاضي **Gomez** قراره في 22 مايو 2000 متضمنا بالطبع اختصاص القضاء الفرنسي بنظر الدعوي، ثم إنه أصدر أمرا لـــ.. **Yahoo** العالمية لكي تقوم بمنع كل ملقمات الانترنت الفرنسية من إمكانية الدخول على خدمات المزاد المثيرة للجدل **Controversial auction services**، إلا إن القاضي **Gomez** لم يتول تحديد ماهية التقنية اللازمة التي يمكن لشركة **Yahoo** استخدامها لكي يمكنها من القيام بتنفيذ أمر المحكمة الوارد في قراره والذي تضمن إمكانية الحصول على مدخل يمكن من خلاله تحديد هوية ملقم الانترنت الذي زار موقع الانترنت المقصود. ولقد تم منح **Yahoo** العالمية مهلة حتى 24 يوليو 2000 لكي تضع أمام المحكمة الحلول التقنية التي سوف تحقق ذلك، ومن ثم تنفيذ القرار المذكور في الحكم، كما قام القاضي الفرنسي بأمر **Yahoo** فرنسا بإزالة كل ربط تصفحي **Navigational links** بـــ.. **Yahoo** العالمية وبث تحذيرات عبر ملقمات **Yahoo** فرنسا حول مسلك **Yahoo** العالمية غير المشروع ، ولقد قضي ايضا بعداد كل من الشركتين مسئولة وملزمة بالتضامن بدفع عشرة آلاف فرنك فرنسي كجزاء لصالح ليكرا واتحاد الطلبة اليهود الفرنسيين.

وفي 24 يوليو 2000 ، قررت **Yahoo** إنه رغم البحث المستمر عن الوسائل التي طلبتها المحكمة فإنه من غير الممكن التوصل الى إمكانية تنفيذ أمر المحكمة المذكور لكون ذلك مستحيلا من الناحية التقنية ، حيث إنه لا توجد الوسائل التقنية الكفيلة بتحقيق أمر المحكمة الصادر بقرارها المؤرخ 22 مايو 2000 ، والذي يتضمن البحث عن الوسائل التقنية لمنع مستخدمي **Yahoo** فرنسا من الولوج الى **Yahoo** العالمية في الولايات المتحدة الامريكية، وبناء على ذلك قام الادعاء باتهام **Yahoo** العالمية بعدم قيامها بما يجب للتوصل، او لتطوير آلياتها، بما يمكنها من إيجاد الحلول التقنية المذكورة، ومن ثم قام الادعاء بتقديم طلب الى القاضي يتضمن تسمية لجنة من الخبراء التقنيين لكي تقرر باستقلالية ما إذا كان هناك إمكانية التوصل الي القيام بتنفيذ قرار المحكمة تقنيا.

وفي 11 أغسطس 2000، وفي تطور مفاجئ، قام القاضي **Gomez** بإصدار قراره بتشكيل لجنة خبراء: ثلاثة خبراء – خبير فرنسي هو **Francois Wallon** خبير مسمى بمحكمة النقض الفرنسية، وخبير أمريكي **Venton Cerf** مكتشف بروتوكول **TCP / IP** (بمشاركة **Bob Khan**)، وخبير اوروبي / إنجليزي **Ben Laurie**) لتقرير ما إذا كانت مثل هذه التقنية يمكن أن تتوافر من عدمه ؟ ومن ثم هل يمكن تنفيذ قرار محكمة باريس المؤرخ 22 مايو 2000؟

وفي السادس من شهر نوفمبر 2000 قامت لجنة الخبراء المذكورة بإيداع تقريرها النهائي بالمحكمة، وتضمن التقرير إن اللجنة انتهت الى امكانية القيام بتنفيذ قرار المحكمة وذلك من حيث توافر الامكانيات التقنية لمنع مستخدمي الانترنت، حيث يتواجدون في نطاقهم الجغرافي الفرنسي، من الولوج الى مواقع الانترنت المستهدفة من التجريم. ولقد اعتبرت لجنة الخبراء استخدام وسائل فلترة او تصفية يمكن ان تحقق الهدف هنا بنسبة 80% بحيث تقيد بنجاح الولوج الى مثل هذه المواقع. وبتاريخ 20 نوفمبر 2000 أصدر

قاضـــي باريس حكمه بإلزام ياهوو بفلترة مســـارها لكي لا يتم بث ما يمكن ان يكون متعارضـــا مع القانون الجنائي[19].

والواقع أن ما قام به القضـاء الفرنسـي انما هو إدانة القدر المتيقن، وهو اسـتضـافة شـركة Yahoo في أحد المواقع المجانية التي تقدمها كخدمة Yahoo auctions للمزاد النازي. بل وأبعد من ذلك فإن تقرير لجنة الخبراء المؤرخ 6 / 11 / 2000 لم يكن دقيقا في أكثر من موقع من حيث كونه تناول أجوبة لأسئلة خاطب بها الخبراء شركة AOL وهي شركة أمريكية قام بتأسيسها أعضاء في المخابرات الأمريكية مما يضفي على الموضوع انعدام الحياد هنا.

ثانياً: فحص النظام الأمني للشبكات: - إن الحاسوب المنفرد غير المتصل بأي نوع من الشبكات stand-alone computer لا يكون عرضـــة للاختراق المعلوماتي إطلاقا، وإنما كل ما يمكن أن يتوافر له هو اختراق مادي، بحيث يتصـل مرتكب الجريمة هنا بالحاسـوب المنفرد اتصـالا مباشـرا، وهذا يجعل عملية الحصـول على الدليل التقني سـريعة وبسـيطة بحيث تتجه الشـبهات الى حائز الجهاز وكذلك كل من قام باستخدامه على نحو او آخر[20].
أما أجهزة الحاسوب المرتبطة بنظام تواصلي عبر شبكات - وكنتيجة لما تقدمه من نشاط معلوماتي متشابك كبيت العنكبوت - فإنها تكون أكثر عرضـة لاسـتخدامها في ارتكاب الجرائم واحتوائها على الأدلة الرقمية، ومن الدارج التأكيد على إن الشـبكات غير المحصـنة بالتشـفير تكون أكثر عرضـة للاختراق وبالتالي فان فحصـها يتطلب وقتا أكثر للحصـول على دليل رقمي هنا، في حين تشكل الشبكات المحصـنة بالتشفير ذات صعوبة أقل في تحصيل الدليل لكون الاختراق يبدو واضحا من خلال الكشف الدوري عليها فيتبين مداه من خلال فحص حركة الدخول هنا [21].

ولعل أكثر النقاط عرضـــة للاختراق هي تلك التي تنطلق من نقطة الاتصـــال بالإنترنت بطريق الهاتف التقليدي Dial up التي تجعلنا نتصـل بالانترنت عن طريق مزود الدخول، فهذه النقطة عرضـة للانتهاك وبالتالي قد تكون موقعا لإثبات الدليل الرقمي على الاختراق.

كذلك إن خاصـية التتبع التصـفحي ID Crack number تتيح لمن يطلع عليها معرفة عنوان الحاسـوب الرقمي IP address، وبالتالي تتبع المسـار المحلي للشـبكة التي تزود حركة التصـفح، ثم التوصـل الى العنوان المادي للمشترك في الشبكة. ومثل هذا الامر يساعد على تقصي الشخص الذي يتعامل مع الحاسوب ويقيم افتراض إن من قام بالتعامل معه انما هو مالكه سيما إذا كان المشترك هنا فردا طبيعيا.

ثالثا: نظام فحص بروتوكول الانترنت: - إن منطق التعرف على الحاسوب الذي تمت مباشرة او ارتكاب الجريمة عبره من السـهولة بمكان، وهذا الامر يطلق عليه عملية التعرف على بروتوكول الانترنت IP، إذ يعد هذا البروتوكول الطابع المميز لاستخدام الانترنت فأي شخص يحصل على بروتوكول الانترنت يمكنه الولوج اليها ليكون عضوا كاملا فيها. يباشر الحركة خلالها ويحصل على خدماتها.

---

[19] انظر الحكم : منشورا عبر صفحة جوريسكوم http://www.juriscom.net بتاريخ 25 نوفمبر 2000 ، كذلك انظر :
Richard Salis, A Look at how U.S Based Yahoo! was Condemned by French Law p . 6 , University of Montreal , November 10, 2000 , available online in nov. 2000 at :
http://www.juriscom.net/txt/jurisfr/cti/yauctions.htm

[20] Testimony of Kevin R. Mitnick / U.S. Senate governmental affairs committee , op - cit

[21] Id.

وعملية البحث في قواعد البيانات لدى مسجلي بروتوكول الانترنت ليست بالمهمة الصعبة، إذ يمكن لأي كان القيام بتحديد حائز هذا او ذاك البروتوكول عن طريق البحث في قاعدة بيانات Whois الخاصة بالمسجلين Registrars فمثلا كان موقع مؤسسة Network Solutions في موقعها www.networksolutions.com يحتوي على عناوين المؤسسات الامريكية حيث تمنح هذه المؤسسة عبر موقعها المذكور نظام استطلاعي لقاعدة بيانات Whois فيها. كذلك يمكن استخدام برمجيات متعددة ومتوافرة عبر الانترنت تقوم برصد بروتوكولات الانترنت[22].

رابعا: فحص الخادم او الملقم: - ويتضمن فحص نظام الاتصال بالإنترنت لزوم فحص الخادم او الملقم، وهو حاسوب ضخم مهمته تحقيق حركة الاتصال بالمواقع والصفحات وكذلك الاتصال المباشر التي يتم استضافتها على هيئة رقمية فيه[23] لذلك نجد إن الخادم يطلق عليه Lieu de stockage des données numerisées . ومن الخوادم ما يكون مهمته ليس تحقيق اتصال مع المواقع والصفحات وانما فقط القيام بتحقيق التواصل مع حلقات النقاش والأحاديث المباشرة او فقط نظام تخزين البريد الالكتروني.. الخ، وبحيث يعمل هذا الخادم على ربط أعضاء الانترنت بغرف التداول والحديث المتواصل فيبرز عضو الانترنت كما لو كان يستضيف من يتحدث معه او البريد الالكتروني.

وتحتاج عملية فحص الخادم في الحقيقة الى ضرورة اتخاذ الإجراءات القانونية اللازمة وفق القانون النافذ في النطاق الإقليمي الذي يوجد فيه بالاضافة الى لزوم الأخذ في الاعتبار مبدأ الغاية من التفتيش وبالتالي خلق مفارقة بين الخادم العام وبين الخادم الخاص المخصص لفئة تراسلية معينة. على إن الامر لا يقف عند هذه النقطة إذ إن تقنية الانترنت تجعل من الممكن القيام بفحص خوادم عن بعد (مبدأ امتداد التفتيش)، وذلك باستخدام تقنية حديثة في هذا الإطار تجعل التوصل الى محتوى حركة الاتصال بالخادم ذات مغزى وربما أفضل من مجرد القيام بفحص الخادم ماديا.

---

[22] **Eoghan Casey - Computer & Internet Crime FAQ - available online in feb 2001 at http://www.forensic-science.com/faq_computer.html**

[23] **TGI Paris, 17Ch. Correc. 28 / 2 / 1999, note: Maitre Stephane LILTI P.3 Disponible enligne a Nov. 1999 a : http://www.legalis.net/jnet/commentaires/lilti_280199.htm**

المطلب الثاني

فحص مركبات الحاسوب

على الرغم من الاهمية التي يتمتع بها الحاسوب في ظل ثورة تكنولوجيا المعلومات، سيما بعد بروز العالم الافتراضي / الانترنت، فإن منطق التعامل التشريعي معه في القانون المقارن كان أكثر حذراً في تعامله مع الحاسوب، سيما حين يتعلق الموضوع بالاجراءات الجنائية وقواعد الاثبات من حيث إنها تعد القواعد التي يقام بمقتضاها التدليل على الجريمة ومرتكبها.

وفي هذا الفرع سوف نتطرق الى فحص مركبات الحاسوب لأهميتها في حركة الإجراءات الجنائية. وربما يعد ضبط الحاسوب أبرز النقاط هنا ومن ثم نبدأ منها.

أولا - مدى لزوم ضبط وحجز الحاسوب Seizure of computer : - يُعد الضبط والحجز بقصد تعقب الدليل الرقمي هو الأسلوب التقليدي في اقامة بنيان هذا الدليل ، وهو يُعد أفضل السبل الى ذلك أيضا[24]، وهذا يستدعي التأكيد على إن الاتجاه الى ضبط وحجز الحاسوب مما يجد موضوعه في مصادرة القطع الصلبة والبرمجيات على السواء[25]، إذ كثيرا ما نجد إن المصادرة موضوع رئيسي في القضايا التي يتم فيها الكشف عن هوية مرتكب الجريمة عبر الانترنت، لكون الانترنت تعمل بنظام استعمال الحاسوب، على أية شاكلة يكون عليها، كالحاسب الشخصي PC او النقال او الشبكات Networks وأيضا الهواتف النقالة التي يدخل عليها الحاسوب فيجعلها تتصل بالانترنت.

ويتم الضبط والحجز هنا بقصد فحص مركبات الحاسوب هذه، والوسيلة الى الفحص هنا هي تفتيش محتوى القطع الصلبة Hardware التي تحتوي برمجيات، بحيث يكون الأسلوب هنا هو التعرف على البرمجيات الموضوعة في هذه القطع الصلبة، وكذلك تلك التي وضعت من ذي قبل وتم الغاؤها، وما إذا كانت هذه القطع الصلبة والبرمجيات تعمل بشكل مضطرد ومتوافق ام أن هناك ما يعيق حركتها، كما لو كان الحاسوب مصابا بفيروس ترتب عليه تعديل في نظامه او هتك لملفات التشغيل او التنفيذ. فمثل هذا الأمر إن حدث يعد عقبة في عملية إقامة بنيان الدليل الرقمي، حتى وإن أمكن التعرف على بعض الملفات التي تشير الى قيام الهاكر مثلا باقتحام موقع من المواقع او التعرف على الشفرات الخاصة به التي أعدها لغزو نظام من الأنظمة المحمية بالقانون.

والواقع إن نظام الضبط والحجز التقليدي يمكن أن يكون محل تطوير في ظل أفكار تكنولوجيا المعلومات، وما ترتب على اعتبارها ثورة. إذ ليس هنا ما يمنع من أن يتم الضبط والحجز عبر الانترنت، وبحيث يتم – في يوم ما غير بعيد – استصدار أمر تفتيش وضبط وحجز (بل ومصادرة) مكونات الحاسوب دون أي تدخل مادي ، وانما يتم ذلك عبر الانترنت، فيقوم مأمور الضبط او الجهة الضبطية بتنبيه مالك او حائز الحاسوب بأذن التفتيش، بل ويقوم كذلك بإجرائه أيضا عبر الانترنت، ثم ضبط البرمجيات والملفات الإجرامية فيه ثم حجزه بوضع اعلان فيه يتم ظهوره على شاشة الحاسوب بمجرد تشغيله بحيث يصعب، إن لم يكن مستحيلا ، تشغيله ، لحين انتهاء التحقيق، والمحاكمة إن استدعى الأمر ذلك. ولقد وجد لذلك مؤشرات في الزمن المعاصر ممثلة في الهيئات النظامية عبر الانترنت مثل **Agence de Protection de Programes**

---

[24] **Peter Sommer , op – cit p. 66**

[25] **USA v. Hay, App 9th Cir. No. 99 – 30101, 24 Oct. 2000. Op – cit .**

(APP) في فرنسا وأوروبا، والتي تغطي نشاط دول الاتحاد الاوروبي سعيا وراء المحافظة على حقوق الملكية الفكرية في المحيط الاوروبي.

ثانيا – التركيبة الصلبة والبرمجية والمعلوماتية للحاسوب : - أشرنا فيما سبق الى إن الحاسوب في ذاته يقوم في تركيبتـه على ثلاثـة أمور هي القطع الصـلبـة Hardware والقطع المرنـة او البرمجيـات Software وأخيرا المعلوماتية Informatiques التي تتوزع ما بين تركيبة البرمجيات والقطع الصلبة ، بحيث يمكن القول إن هناك أمرين على درجة من الأهمية في إطار الحاسـوب وهما إن الحاسـوب ليس له تلك القيمة التي هو عليها إذا لم يكن هناك برمجيات تحرك مكنونه الصـلب ، إذ بدون هذه البرمجيات يكون مجرد قطع معدنية وبلاستيكية وخشبية لا يمكن الاستفادة منها ، هذا من ناحية . ومن ناحية اخرى فإن الذي سـلف يعني ان تلك القطع الصـلبة تحتاج منطقيا الى البرمجيات لكي يمكن التعامل معها، فالبرمجيات هى التي تقوم بتحويل تلك القطع الصـلبة الى مادة يمكنها التعامل مع مطلب انسـاني ما بحيث تعطي جوابا عن كل سـؤال. ولا يقف الامر عند هذا الحد بل ترتبط حاجة القطع الصـلبة بالبرمجيات الى منطق المعلوماتية القائم على أسـاس حرية تجول المعلومات في الحاسـوب ذاته ، وهو مبدأ يعني إن ما يفهمه الحاسـوب هو منطق يتعامل مع الحرية بشكل لا ينتمي الى تفسير الحرية الملتزمة التي يعتمدها القانون ، وانما ينطلق من تعامله مع كل ما يمكن إدراجه فيه من معلومات ، وعلى النحو الذي لا يميز بين هذه المعلومة وتلك، وفي هذا ما يجعلنا نؤكد على إن التمييز الحادث بين المشـروعية و اللا مشـروعية في اطار الاجرام المعلوماتي انما مبعثه القانون وليس التقنية ، ثم ان هذه المفارقة التي يقيمها القانون هدفها ليس البرمجيات، وانما ما تحتويه من معلومات سـواء جاءت في شـكل كتابة او رسـوميات او مسـموعات او مرئيات ...الخ ، ذلك إن البرمجيات التي يمكن أن تحتوي معلوماتية غير مشروعة يمكن استخدامها كليا او جزئيا(بطريق الاشتقاق مثلا) لكي تعمل عليها نظم معلوماتية أخرى مشروعة.

وإذا كان الحاسـوب على النحو السـالف في تكوينه، وبحيث يمكن بالتالي تفتيش وضـبط القطع المرنة التي تتكون من برمجيات بما تحويه من بيانات، فإن ذلك يقودنا بالضـرورة الى بحث مدى إمكانية ضـبط وحجز القطع الصلبة التي يتشكل منها الحاسوب، ومدى الحاجة الى القيام بهذا الإجراء؟

والحقيقة أن النظم التقليدية تستدعي بالضـرورة القيام بعملية الضـبط المادية المذكورة بحيث يمكن الاستفادة من النظم التقليدية في هذا الإطار ، ومثل هذه النظم التقليدية قد لا يبدو مثل هذا الإجراء مفيدا حال القيام بإجراء ضـبط عن بعد ، فيما بين الدول مثلا او خارج نطاق الحدود الإقليمية للدول ففي مثل هذه الحالات يمكن الاكتفاء بإجراء عمليات الضبط الرقمي الممثلة في ضبط وحجز البرمجيات والبيانات عبر الحاسوب بحيث لا يكون من السهل على المالك او الحائز مرتكب الجريمة استخدامه الى حين وصول جهات الضبط القضـائي او السلطات العامة. بل ويمكن باستخدام أسلوب الضبط والحجز الرقمي القيام بمطالبة الحائز او المالك بتسليم الجهاز الى أقرب جهة عامة.

وعندنا أن التطور يمكن أن يقود الى مثل هذا الأمر، أي الفحص المعنوي دون المادي، ولكن مع ذلك فإن متطلبات المحاكمة العادلة تستلزم أن يكون الفحص ماديا، كما المعنوي للارتباط القائم في شكل طبيعي بين مكونات الحاسـوب ككل. وذلك ضـمانة لازمة عندنا حتى تتوافر للمتهم ضـمانات المحاكمة الكاملة التي صارعت الإنسانية مراحل طويلة في مسيرتها للحصول عليها.
لذلك فإننا هنا سـوف نتطرق الى فحص المكونات المادية والمعنوية او الرقمية على السـواء توصـلا الى رصد قيمة هذا الفحص فيما ينجم عنه من أدلة.

ثالثا ـ كيفية فحص مركبات الحاسوب: ـ تعتمد عملية الفحص هنا على الحاسوب أيضا سواء بالفحص الذاتي للحاسوب، وهو قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك الى طالب الفحص، ومثل هذه الحالة يجب ألا يقوم بها الهواة او المستخدمون العاديون حيث تتطلب مثل هذه الحالة قدرات تقنية عالية.

وقد يتم الفحص بطريقة الاستعانة بحاسوب آخر وأجهزة تقنية عالية متخصصة في بحث جزئية او جزئيات عبر الحاسوب ، فمثلا قصف نظام معلوماتي في نظم حاسوب تشغيل الطيران المدني[26] وحواسيب المستشفيات او بورصة المعلومات NASDAQ ومؤسسات الخدمة المدنية وما تحويه من بيانات اسمية، وكذلك تداول الملفات التي تحوي معلومات خطرة مثل الفيروسات وتبادل صور الدعارة، ودعارة الأطفال على الخصوص، يمكن من خلال تلك التقنيات القيام برصدها، وحديثا أمكن لمؤسسات كبيرة مثل Actis Technology , Orange Telecom في بريطانيا القيام باعداد برمجيات راصدة لمثل هذه الحالات.

أ: فحص القرص الصلب: ـ يعد القرص الصلب المحتوى الذي يضم في داخله مجموع البيانات الرقمية ذات الطابع الثنائي، والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (0 – 1) الذي يتكون منه تفصيل البيانات المذكورة[27]. ويشير العلماء الى امكانية القيام بفحص كلي او جزئي للقرص الصلب.

والفحص الجزئي للقرص الصلب The molecular analysis of a hard disk يؤدي الى التعرف على محتوى البيانات ثنائية الرقم، والتي يؤدي التعامل معها الى الكشف على القيمة الاسترادادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة او صور او أصوات أو.. الخ. وكذلك ما تم حذفه Delete من بيانات وبرمجيات وبرامج. وعملية الإلغاء او الحذف بطبيعة الحال تحتاج الى برمجية خاصة للقيام بها، فليس الامر مرتبطا بقطعة صلبة وانما ببرمجيات ايضا [28] ، والمثال التقليدي المستخدم هنا هو حالة البحث في ملفات النسخ الإضافية التي تحتويها نظم التشغيل مثل النوافذ مثل ملفات Temp و Internet temporary file .. وهذه الأخيرة ملفات تأخذ نسخا احتياطية من كل صفحة يتم الولوج اليها عبر الانترنت، كذلك توجد في نظم التشغيل ملفات خاصة بالإنزال Download file مهمتها استقبال الملفات التي يتم تحميلها على الحاسوب من خارجه وعبر الانترنت. فهذه الملفات جميعها مركزها القرص الصلب بطبيعة الحال حتى في ظل رصد أماكن اخرى تحتوي برمجيات مثل المعالج Processor الذي يتم تصنيعه وتلقينه ببرمجيته في ظل ظروف خاصة بحيث يمكنه القيام بدوره في الحاسوب.

ب: فحص البرمجيات: ـ ويتم التمييز هنا بين حالة الفحص الداخلي للبرمجيات وحالة الفحص الخارجي لها.
ففي حالة الفحص الداخلي ، ويتم من خلال بحث البناء المنطقي للبرمجية بما يوحي بأن هناك مجهودا تجديديا في اعداده للعمل Setup حين انزاله في الحاسوب Installation ، وذلك من الأمور التي يدركها الخبراء من حيث استلزام الربط الصحيح في البرمجية ذاتها، وبحيث يلزم المبرمج تتبع الخطوات المنطقية التي تعبر عن جهده التجديدي، سيما وإن الخبراء على دراية بكيفية البرمجة والخيارات المتعددة [29]، وأكثر

---

[26] **Airport flight management computers**

[27] **TGI Paris, 17Ch. Correc. 28 / 2 / 1999 op -cit**

[28] **Marcus Gibson- op – cit**

[29] **جالر – المرجع السابق ص. 81**

ما يتم العمل في اطار الفحص الداخلي هو في البحث عن مصـــدر الملفات الموجودة في هذا الاطار، إذ إن النسـخ عبر الانترنت لا يعد مشـابها في هذا الشـأن مع القيام بنسـخ المؤلف باسـتخدام برمجيات معالجة الكلمات Word Processing. فالأول نسخ تم عبر العالم الافتراضي في حين أن النسخ الثاني تم باستخدام مصنف متداول في العالم المادي.

وإذا كانت الوسـيلة التي تم بها النسـخ ليسـت ذات أهمية في هذا الاطار إلا إنها – على أية حال – تفيد في ترتيب كيفية حدوث الجريمة، وقد يقود مثل هذا الأمر الى التوصـــل الى جرائم أخرى، كما لو كان هناك صور داعرة في الحاسوب فإن الكشف عما إذا كانت جذورها عبر الانترنت ام في الواقع المادي من خلال مسـح صـــور فوتوغرافية، يمكن أن يقود الى مروجها في العالم المادي او القبض على شـبكات الدعارة والرقيق الابيض او دعارة الأطفال ... الخ ، او أن يتم التعرف على الكيفية التي تم بها اعداد مثل هذه الصـور كما هو الشـأن في اسـتخدام برمجيات الرسـوميات لوضـع رأس أمراءة او فتاة على جسـد عار (تزييف الصـور) بما يمثل مشـكلة او أخرى لصـاحبة الرأس. إذ يمكن التوصـل الى الحقيقة دائما باسـتخدام برمجيات معقدة نوعا ما (كونها لا تزال حديثة فقط).

أما في حالة الفحص الخارجي، فان اخطر قاعدة يمكن الاســتفادة منها هنا هي ما يطلق عليها فقها (هناك دائما دخان يلحق عملية اطلاق النار) للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة، ويتم تطبيقها حين التطرق هنا الى البناء المنطقي للبرمجية فيما إذا كانت منسوخة مثلا، وفي هذه الحالة يتم اللجوء الى النسخة الأصلية للمقارنة بينها وبين النسخة المسروقة، فقد حدث في قضية معهد SAS ضد S&H حيث تم ترك جزئية غير موظفة في برمجية SAS تركت دون سبب محدد وتم نسخها من قبل S&H اثناء نسخ جزئية من البرمجية ولقد اعترفت S&H بهذا النسخ أثناء المحاكمة[30].

ج: خطورة البرمجيات المعطوبة Software defects: - ولعل من اللازم التطرق الى موضـــوع أهمية فحص البرمجيات عبر الحاسوب. ذلك إن برمجية الحاسوب ليست ذات نظرة مثالية حسبما عرضنا لذلك آنفا، إذ يظل دائما هناك قصـور- ولو جزئي- في هذه البرمجيات يمكن أن يؤثر في الحاسـوب فيجعله محل شـك يمكن ان يهز قيمتها كدليل. هذا القصـور له أثره في عملية تقييم الدليل المسـتمد من البرمجية ذاتها، فمثلا إن استمداد أدلة حين فحص برمجية معينة (كبرمجية بريد الكتروني او برمجية اتصال بمواقع دعارة او برمجية تحصـيل أموال مخدرات او برمجية العاب قمار.. الخ) مركبة على الحاسـوب، فإن مجرد كون هذه البرمجية معطوبة لسبب من الاسباب يجعلها قاصـرة عن استمداد دليل يحمل الادانة، حتى وإن أمكن اســتخدام برمجيات عالية الكفاءة لتنقيتها من الشـــوائب، إذ يظل حالها محل شـــك، لذلك تعد البرمجيات المعطوبة في مستوى عناصر الاستدلال وليست دليلا كاملا.

ويمكن التدليل على ذلك بما هو معروف من موضـوع النسخ الأولية او المبدئية Shareware او Beta والتي تطرح في الاســواق مجانا ، والظاهر من هذه الظاهرة هي تعريف المســتهلك النهائي بهذه او تلك البرمجية او المنتج الرقمي ، إلا إن الأســباب الخفية في هذا الاطار كما يقرر المبرمجون من حيث كونها تسبب مشكلات في الحاسوب ذاته فضلا عن كون هذه البرمجيات لم توزع باسلوب مجاني إلا لمعرفة الخلل البرمجي فيها ، والذي يتم التعرف عليه بإنزالها الى التداول لمدة زمنية معينة يتم خلالها استقبال الشكاوى من المسـتهلكين لكي يتم إصـلاح الخلل فيها[31]. ومثل هذا الأمر يمكن أن يجعل البرمجية محل شـك في هذا الاطار ، وهو شـك كاف لهدم الدليل إذا تصـاعدت المشـكلة الى أخطر من هذا الأمر ، حين تكون البرمجية

[30] جالر ص. 81

[31] Louis Longdin - Liability for defects in bespoke software: are lawyers & information scintists speaking the same langguage? - P. 11 , International journal of law & technology vol. 8 issue 1 , Oxford UNI. Press 2000 .

ليست مجرد برمجية أولية او مؤقتة وانما أيضا برمجية كاملة يتم ابتياعها ويتم استخدامها في جريمة ، ويتبين حين فحصها باعتبارها موضوعا لهذه الجريمة إنها معطوبة او إنها مرتبطة ببرمجية معطوبة إذا كان إنزال إحداهما يجعل من اللازم ارتباطها بنظام التشغيل المحمل على الحاسوب ، لكون نظام التشغيل يشكل أساس عمل المبرمجين ، مما يعني إن الارتباط يكون واضحا بين البرمجية ونظام التشغيل، وهو ما يبدو واضحا في اعتماد المبرمجين على واجهات التطبيق Interface السائدة في نظم التشغيل[32].

إن مسألة العطب البرمجي تُعد من المسائل الخطرة في إطار فحص البرمجيات، لكون الاتصال بالانترنت عبر الحاسوب يستلزم وجود برمجيات محملة فيه. إذ إن الحاسوب دون برمجيات يظل دائما مجرد قطع صلبة. ومع ذلك فإن هذه الخطورة لا يمكن التعويل عليها في كل الأحوال، إذ يختلف الاستناد إليها من حال الى حال ، وبحسب الوضعية التي يعمل بها الحاسوب، إذ يمكن مثلا الاعتماد على الحالة العادية التي يستخدم فيها الحاسوب للتعويل على الدليل المستمد منه، حتى ولو كان الحاسوب ذاته مصابا بنوع من العلل التقني نتيجة لوجود برمجية او مجموعة برمجيات معطوبة، ذلك إن تحديد درجة العطب يمكن القول باختلافها من مكان الى أخر ومن دولة الى أخرى ، فمن الصعوبة بمكان القول هنا بعدم إمكانية التعويل على دليل رقمي لمجرد إن الحاسوب يحتوي على برمجيات معطوبة ، فمثل هذا القول لا يمكن قبوله إطلاقا ، وانما وفقا للحالة العادية التي The Regular Statute التي يعمل بها الحاسوب ، بحيث لا يتم التعويل على الدليل المستمد من حاسوب محاصر تماما بالعطب البرمجي ، أما اذا كان العطب البرمجي يجعل الحاسوب ، مع ذلك ، مؤهلا للعمل عليه فإن مثل هذا العطب البرمجي لا يؤثر في قيمة الدليل ومدى قبوله أمام المحاكم في هذا الشأن[33] على استثناء يتعلق بالبرمجية المعطوبة ذاتها حيث لا يقبل الدليل المستمد منها او ذي العلاقة بها.

د: شرط سلامة الحاسوب: - إن شرط سلامة الحاسوب يعني صحة حركة القطع الصلبة Hadware فيه، بحيث يجب أن تعمل بطريقة عادية، مثلما هو الحال في أي حاسوب آخر من ذات التركيبة، وبحيث يجب فحص حركة الحاسوب المذكورة لكي يمكن تجنب الوقوع في مأزق رفض المحكمة الاعتداد بالدليل المنبثق عنه. وفي القضاء المقارن فأن شرط سلامة الحاسوب مطعن رئيسي على كل دليل تم الحصول عليه بحيث يجب الكشف على حركة الحاسوب بداية والإقرار بسلامته، وذلك منذ قضية Rosenberg v. Collins حيث قررت المحكمة قبول الدليل الرقمي إذا كان مستمدا من حاسوب سليم[34].

هـ: فحص النظام المعلوماتي: - يعني فحص النظام المعلوماتي ضبط كافة ما يحتويه الحاسوب من معلومات يمكن استردادها عبره تكون مخزنة في ملفات Files على أية شاكلة يمكن أن تكون عليها الحركة الاسترادية، ما دام موضوعها يشكّل جريمة. ويلزم هنا التطرق الى فكرة المحتوى المعلوماتي للحاسوب حتى يمكن فهم الكيفية التي يلزم أن تتم فيها عملية فحص النظام المعلوماتي.

إن النظام المعلوماتي للحاسوب لا يحتوي على معلومات كما هو المعتقد السائد لدى الكثيرين. وانما المحتوى المعلوماتي عادة ما يتكون من بيانات ثنائية الهيئة الرقمية يتم إيداعها في الحاسوب، وهذا الإيداع

---

[32] **Id. at 8**

[33] **Orin S. Kerr – Computer Records & the federal Rules of Evidence , USA Bukketin March 2001 P. 6 , US DOJ, Vol. 49 No. 2 , available online in Dec. 2001 at http://www.cybercrime.gov**

[34] **The hand book of Information Security Management : Law, Investigation, & Ethics - available online in feb. 2001 at: http://secinf.net/info/misc/handbook/555-558.html**

يأخذ شـــكل تخزين Stockage [35]. وهذه البيانات يقوم الحاســـوب بمعالجتها ويبرزها على هيئة معلومة محددة، حين يتم استدعاؤها من قبل الغير او أي مستخدم للحاسوب، وما دام لم يتم استدعاء معلومة محددة فإن بياناتها تظل في حالة تخزين في الحاسـوب. وتلك نقطة على درجة كبيرة من الأهمية إذا تأملنا فكرة إن ما يوجد من معلومات في الحاسوب إنما تتكّون حال قيام الغير باستدعاء أي منها تحديدا، فلا يقوم الحاسوب باســـتدعاء كافة المعلومات مرة واحدة. ومن ثم يجب بداية أن يتم تحديد المعلومة المراد اســـتدعائها من البيانات المختلفة المخزنة في الحاسوب لكي تظهر لنا بعد ذلك.

وبطبيعة الحال إن كل نظام معلوماتي تكون مهمته الأساسية تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب Computer User ، فالنظام المعلوماتي على هذا النحو يتسع مفهومه لكي يشمل كل المعلومات التي يمكن أن تكون مفيدة ، في الوقت الذي يحتوي أيضـــا نظاما ذاتيا لتخزين البيانات فيه ، وطرائق التخزين متعددة الأشـكال في كل نظام حاسـوبي بحيث يمكن التمييز بينها في عملية الحفظ العادية التي يمكن إجرائها بكل سهولة باستخدام خاصية الحفظ Save العادية في البرمجيات المتداولة ، ثم إنه من الممكن أن تكون خاصية الحفظ متوافرة في شكل استخدام حاجز مرور او كلمة سر بحيث لا يمكن الدخول الى أي من الملفات المخزنة سوى باستخدام كلمة المرور المذكورة.

كذلك فإنه في نظم الشبكات فإن عملية تخزين البيانات فيها تحتاج من السلطات لزوم التحرك السريع لضبط الأدلة، إذ إن في الكثير من الحالات يقوم مزودو الشبكات باحداث تصفية مستمرة لما تحتويه الشبكات من بيانات ذات قيمة استردادية.

والحقيقة أنه لا يمكن للحديث عن فحص النظام المعلوماتي وطرائق تخزين البيانات في الحواســـيب أن ينتهي، إذ على حسـب كثرة التعامل بالحاسـوب يتكاثر محتوى النظام المعلوماتي، سـيما إن نظم المعلومات تتعامل مع بعضها البعض عن طريق برمجيات متخصصة ومتوافرة دون تدخل الانسان. لنتخيل إن عملية فحص نظام معلوماتي في أحد الفنادق للكشـــف عن جريمة قتل، إذ إن مجرد معرفة عدد التعاملات مع هذا النظام المعلوماتي في خلال اسبوع واحد فقط قد تصل الى ملايين الرسائل ما بين الاطلاع على الحجوزات والاتصـــالات التي تمت والمحادثات الهاتفية وطلبات خدمات الغرف وطلبات المقهى او المقاهي والمطاعم وحركة الخروج والدخول ... الخ. إن الصـــعوبة تزداد هنا إذا أدركنا إن فحص مركبات الحاســـوب ربما تكون الامل الوحيد في التوصـــل الى مرتكب الجريمة. والصـــعوبة هنا تزداد أكثر فأكثر إذا علمنا إنه قد مضـــى قد طويل على ارتكاب الجريمة او حين مطاردة شـخص كان قد أمضـــى عدة أيام في هذا الفندق في فترة مضت وهو في سبيل إعداد العدة لارتكاب الجريمة، إذ إنه في بعض الجرائم يكون هناك التزام قانوني على سلطات التحقيق الإجابة على كافة الأسئلة التي يمكن ان تطرح عليها في المحكمة.

لذلك يعد النظام المعلوماتي على درجة من الخطورة، وهذا يستدعي حين ضـبط وحجز الحاسـوب التعرف على كنهه وطريقة عمله ونوعية الملفات التي يتم التعامل بها فيه ونوعية نظام التشـغيل الذي يقوم عليه هذا النظام، وفيما إذا كان نظام تشغيل خاص ام انه متداول.

ولا تتخذ عملية تخزين البيانات شكلا محددا وانما تتنوع أساليب التخزين، والتي تصل مداها الى حد إمكانية وضـع او تخزين البيانات بشـكل آمن في الحاسـوب او مجموعة حواسـيب Storing Data Securely، بنظام التشـــفير Encrypted data مثلا او بنظام إخفاء البيانات المعلوماتي Steganography او

[35] TGI Paris, 17Ch. Correc. 28 / 2 / 1999 op –cit

Information Hide، بحيث لا يظهر لنا الملف على الإطلاق حتى في حالة البحث الآلي للحاسوب عن هذه النوعية من الملفات، التي قد تحتوي مواد إجرامية وتفوت الفرصة – بسبب هذه التقنية – على المحققين من الوصول إليها [36] .

ومن الممكن أيضا أن تكون هذه التقنية تحتاج الى الحذر الشديد حين التعامل معها سيما إذا كان نظام الإخفاء هنا يحتاج الى كلمة مرور او مفتاح فك التشفير.. الخ [37] .

و: فحص نظام ذاكرة التخزين Caching: - يعد نظام ذاكرة التخزين Stockage من مزايا نظم تشغيل الحاسوب تحديدا. وكلما كان نظام التشغيل متطورا كان نظام ذاكرة التخزين أكثر دقة. وإذا كنا قد عرضنا لنظام التخزين بشكل مستقل عن النظام البرمجي، فإن ذلك عائد الى خطورة هذا النظام، حيث إنه يشّكل أحد المقدمات الكبرى الى فحص نظام الحاسوب ومركباته.
ويمكن تعريف نظام ذاكرة التخزين بأنه **"قدرة الحاسوب الآلية على الاحتفاظ في ذاكرته بنسخة كاملة مما اطلع عليه عضو الانترنت أثناء إبحاره عبر العالم الافتراضي"**[38].

وفحص نظام التخزين في الذاكرة يعد من الأماكن الهامة حين القيام بفحص نظام الحاسوب لمعرفة ما تم زيارته عبر الانترنت. وتسمح الأنظمة الجديدة بمتابعة ما تم زيارته لفترة زمنية طويلة، حتى وإن كان عضو الانترنت قد قام بحذف كافة ما قام نظام التشغيل بتخزينه، كذلك يمكن باستخدام برمجيات معينة القيام باسترجاع رحلة الحاسوب خلال عملية التصفح لفترات طويلة من الزمن قد تصل الى ستة أشهر كاملة. ويمكن الاستفادة من نظام التخزين هنا في حالات التلبس كونه يمكن من التعرف على حالة الإبحار عبر الانترنت، حتى وإن قام المشتبه فيه بإغلاق الاتصال Disconnected الاتصال بالإنترنت. كل ذلك ما دام نظام التشغيل لم يتم حذفه من القرص الصلب بالطبع، وإن كان هناك برمجيات قوية لدى بعض المنظمات الشرطية في العالم تسمح باستطلاع القرص الصلب، حتى في حالات التخلص من محتوياته باستخدام خاصية الإزالة الكلية.
ز: فحص الطابعة: - يمكن رصد الحركة الخارجية سعيا وراء الدليل التقني بفحص الطابعات سيما الحديثة منها، إذ تتضمن الطابعات الحديثة ميزة تخزين منطقية لمجموع الصفحات التي تم استخراجها من

---

[36] **Ian Brown & Brian Gladman – The Regulation Powers Bill – Technically inept: ineffective against criminals while undermining the Privacy, safety & security of honest citizens & businesses – P. 4 Available online in june 2001 at http://www.fipr.org/rip/RIPcountermeasures.htm**

[37] **Id.**

[38] **M. Hubert BOUCHET- LA CYBERSURVEILLANCE DES SALARIES DANS L'ENTREPRISE - RAPPORT D'ETUDE ET DE CONSULTATION PUBLIQUE - Mars 2001 – P. 12: . La mémoire cache: L'utilisation de la mémoire cache est un moyen d'optimiser les temps de chargement et désengorger le réseau. Son principe est analogue à celui du proxy évoqué ci-dessus : éviter de solliciter inutilement les serveurs distants de site web quand l'internaute consulte fréquemment les mêmes pages. Mais à la différence du proxy qui est sur un serveur externe, ici les pages sont mémorisées sur le micro de l'internaute au fur et à mesure de leur consultation. Si cette fonctionnalité est présente sur le navigateur, lorsque une requête est lancée, le navigateur commence par aller voir sur un répertoire du disque dur si la page HTML demandée n'aurait pas été chargée auparavant. Si tel n'est pas le cas, il effectuera alors la requête auprès du proxy, puis auprès du serveur distant, mais lorsque son résultat arrive, il sera enregistré sur le disque en même temps que présenté à l'écran. La fois suivante, si la même requête est lancée, le navigateur ira simplement la lire sur le disque. Cette mémoire est très souvent appelée "Temporary Internet Files" ou "cache" dans l'arborescence du disque dur. La rubrique "Vos traces" sur www.cnil.fr explique aux internautes comment effacer leurs traces, s'ils le souhaitent.**

الحاسوب، حتى في الحالة التي يكون هذا الملف قد تم إلغاؤه Deleted. وفي هذه الحالة الأخيرة يتم استخدام برمجيات متطورة لاسترجاع ما تم اتخاذه من أوامر عبر الحاسوب، ومنها أمر الطباعة، فتقوم الطابعة بطباعة ما قامت في فترة زمنية سابقة بطباعته، وهو أمر بالضرورة يؤدي الى الحصول على مخرجات الطابعة Hard Copy Printout التي تفيد في كشف الحقيقة. والجدير بالملاحظة في هذه البرمجية انها تتضمن حيزا لكي يوضع فيه تاريخ اليوم المراد تقصي قيام الطابعة بعمل ما فيه، حيث إنها تعمل على استرجاع النظام التاريخي History المتطور في متصفح المستكشف Explorer 5.5 من Microsoft، حين إنها لا تعمل على متصفح أقدم او أي متصفح آخر.

فمثل هذه البرمجيات تساعد في معرفة ما إذا كان الشخص قد قام بطباعة صفحات تتضمن صور داعرة وخليعة من الانترنت، وتاريخ قيامه بذلك وساعته، بدقة غريبة. كذلك في الجرائم الاخرى من ذات النوعية يمكن مثلا التعرف على عدد النسخ التي تم طباعتها في موضوع العدوان على حقوق المؤلف، كما يمكن أيضا معرفة تاريخ وساعة القيام بذلك والمدد المختلفة التي تم فيها ارتكاب هذه الأفعال.

ويراعى إن تقدير ما إذا كان مالك الحاسوب او الهوية عبر الانترنت هو مرتكب الجريمة عبر الانترنت، وإن ما تم تخريجه بالطباعة Printouts منسوب إليه يظل خاضعا لتقدير محكمة الموضوع في كل الأحوال. فلا يمكن مثلا عرض ما هو مخزن في الحاسوب من ملفات على خبير خطوط كما هو الشأن في الكتابة العادية باستخدام القلم، ويظهر ذلك جليا حال وجود الشخص في غرف مناقشة ويقوم بالتعريف بنفسه وشخصه وهويته الحقيقية، ثم يقوم الخبير باسترجاع ملف التخزين الخاص بالحديث المذكور وطباعته على الطابعة بغرض تقديمه الى محكمة الموضوع، ففي هذه الحالة لا يمكن التعويل بدقة على إن ما هو موجود بالملف من كلام مدون منسوب لمالك الحاسوب ما لم يكن هناك اعتراف لاحق من قبل المالك او المستخدم الذي تم ضبطه [39] .

ح: فحص لوحة المفاتيح: - يمكن أن تكون لوحة المفاتيح keyboard محلا لفحص خبراء تكنولوجيا المعلومات في المعامل الجنائية. حيث إن لوحة المفاتيح الحديثة كثيرا ما يتم استخدامها كملقم او خادم وهمي من قبل الهكرة، وفي هذه الحالة يكون التعامل معها كأداة او وسيلة مساعدة في ارتكاب الجريمة، ومن ثم يمكن عداد الدليل المستمد منها دليلا يساعد في إبراز حقيقة الواقعة الإجرامية.

ط: فحص النظام الأمني البرمجي لأنظمة الحاسوب: - تعد الأنظمة الأمنية المشيدة في الحاسوب المنفرد، وبحيث يكون غير متصل بشبكة ما من أفضل السبل التي تجعله في مأمن من امكانية ارتكاب جرائم فيه[40]. على أن مثل هذه النظم الأمنية المنفردة قد توحي بنوع من الخصوصية التي تستلزم الكشف عن مقومات هذا الجهاز المنفرد، إذ إن الخصوصية المطلقة هنا يمكن أن تكون عاملا سلبيا في رفض تمكين الغير من الإطلاع على محتوى هذه الأجهزة، وبالتالي تشكل عائقا يمنع الغير أيا كان من المتابعة والتقصي عن الأعمال التي يقوم بها مستخدم الجهاز. ومثل هذا الأمر يتوافر بكثافة في المؤسسات التي تستخدم الحاسوب في أعمالها، ومن ثم فإن إقامة مثل هذه النظم في أجهزة الحاسوب يمكن أن تكون مانعا من التوصل الى الأدلة الرقمية. لذلك فإن فحص مثل هذه الأجهزة يعد من اللزوميات في هذا الشأن. ولا يستلزم مثل هذا الفحص هنا ضرورة حضور مالك او حائز الجهاز هنا، حيث تتوافر القدرات العملية في معرفة بل وكسر كلمات المرور.

---

[39] **Orin S. Kerr – Computer Records & the federal Rules of Evidence, op cit at 7**

[40] **Testimony of Kevin R. Mitnick / U.S. Senate governmental affairs committee, op - cit**

كذلك إن تقدما حدث في اطار فحص النظام الأمني للحاسوب ممثل في فحص نظم تشغيل الحاسوب OpSys وهو البرمجية التي تعد السيد المطلق للحاسوب حين يكون في حالة عمل، فهو عبارة عن مجموعة من البرمجيات المختلفة التي تتحد فيما بينها في اطار برمجية تنفيذية كبرى (تعمل كمدير مشروع) حيث تعد هذه الأخيرة البوتقة التي تستقبل الأوامر وتقوم بتحليلها وتوزيعها على البرمجية الصغرى التي تقوم بتنفيذ هذا الأمر[41]، حيث يتحكم في وظائف عمل الحاسوب وكيفية وضع المعلومات في أطر معلوماتية متواصلة وكيفية استرجاعها، وكذلك يتحكم في النظام التوزيعي للذاكرة ...الخ. ونظم التشغيل في عمومها تحتوي ثغرات في عملية بنائها قد تكون متروكة كذلك لسبب او أخر، ومن هذه الأسباب إمكانية التعامل مع نظام التشغيل بقصد تطويره او إصلاح الخلل الذي يتم التعرف عليه بعد إطلاقه في السوق، فمثل هذه الثغرات، وحتى يتم التعرف عليها، يمكنها استقبال الانتهاكات وبما يشعل البحث في نظم التشغيل التي تم وضعها على الحاسوب وتاريخ تركيبها بل وتاريخ ورقم إصدارها، مؤديا الى معرفة الكيفية التي تم بها الاختراق مثلا وبما يتوافق مع العيوب التي تعتري هذه النظم.

كذلك توجد إمكانية من خلال البحث والتقصي في مركبات الحاسوب التوصل باستخدامات برمجيات مخصصة الى وجود برمجيات عابثة، وهي يطلق عليها مصطلحات عدة أبرزها البرمجيات الشريرة Rogue software programs ، وكونها شريرة فإن ذلك منطلق من دورها الوظيفي حيث تكون مهمتها محددة بشكل ملفت للأنظار ، مثلما هو الحال في برمجيات كسر كلمات المرور ، وكذلك برمجيات الاختراق التي يستخدمها الهكرة في احداثيات التواصل بين الشبكات بعضها البعض ، حيث تقوم هذه البرمجيات بوضع أبواب خلفية back doors في البرمجيات التي تتعامل مع الشبكات و الحواسيب، بما في ذلك نظم التشغيل، حيث تكون الصفحة الخاصة عبر الانترنت مرتبطة بهذه البرمجية، كما هو الشأن في وضع باب خلفي في صفحة البريد الالكتروني مجاني (واقعة hotmail.com مثلا) حيث تجعل المخترق يضع فقط أسم المتعامل بالبريد الالكتروني دون حاجة لوضع كلمة السر او العبور .

ومن الأمور التي تسمح بانتهاكات في مجال برمجيات الحاسوب عدم تطوير upgrade نظم الحاسوب، حيث إن عدم تطويرها يسمح باتساع إدراك الهكرة لمقومات التعامل مع النظم القديمة، وفي هذه الحالة يكون الباحث عن الدليل الرقمي أمام مهمة أسهل بكثير حين تعامله مع جهاز يحتوي برمجيات قديمة، عما هو عليه حاله حين يتعامل مع برمجيات متطورة او تم تطويرها، إذ في الحالة الأخيرة يكون تعقب الدليل الرقمي من الصعوبة بمكان. ففي حالة البرمجيات التي لم يتم تطويرها يمكن معرفة تحركات المخترق مثلا وأين يمكن أن يكون تاركا بصمته الالكترونية، والمناطق الأخرى التي يجب عليه المرور بها لكي يتم جريمته، في حين إن البرمجيات المتطورة تجعل الأمر أكثر صعوبة على الجاني، سيما إذا كان التجديد في تلك البرمجيات يحتوي على تطوير في نظم الملاحقة والأمن فيها. إذ أمكن تطوير برمجيات التصفح مثلا لكي يمكنها استنساخ نسخة من كل موقع يتم الولوج اليه عبر الانترنت ويتم حفظ هذه النسخ في الحاسوب، الذي تم تركيب هذه البرمجية عليه في نظام التشغيل Windows (internet temporary files)، كذلك هناك بعض البرمجيات التي يتم اعدادها في نظم الشبكات، بحيث تقوم بحفظ نسخة من الصفحة حال التصفح عبر الانترنت وبحيث يتم حفظها في خادم خاص معد لهذا الأمر.

[41] **Id .**

الفصل الثاني
الخبرة التقنية

إن التطور التقني في الانترنت سوف يقود الى تغيير كبير، إن لم يكن كليا، في المفاهيم السائدة حول الدليل. ويؤدي هذا القول حقيقة الى اعلان انضمام الخبرة التقنية إلى عالم الخبرة المتميز بتصنيف التعامل مع موضوع الدعوى، من حيث ضرورة الاستعانة بالمتخصص في مجال النزاع، وهذا الامر يتطلب التعرف على نظام الخبرة من حيث متطلبات صحتها هنا. وهو أمر يلجأ إليه القاضي بحكم النظرة التي تكاد تكون طبيعية إلا أنها تقليدية في الحقيقة وليست طبيعية.

إن الخبرة القضائية- حتى الآن- تستدعي توافر ركني لها، ركن شكلي وآخر موضوعي. وإذا كان الركن الموضوعي مقدرا له قدر من الحرية العلمية يكون الخبير فيها مستخدما لأدواته العلمية والعملية، التي بمقتضاها ينطلق الى وضع الاجابة على المعضلة الفنية محل سؤال القضاء، فإن الركن الشكلي فيها ، الذي يمثل التخصص في مستوى الدراسة والعلم الذي اكتسبه، ينبغي أن يكون مقننا من قبل مؤسسة علمية معترف بها كجامعة او معهد او غير ذلك، وهذا يعد ركنا أساسيا في هذا المجال، بحيث سار التقليد القضائي في هذا الإطار على ضرورة اللجوء الى الخبرة المتوافر فيها هذان الركنان.

فالخبرة الحسابية تستدعي خبيرا حسابيا وماليا، والخبرة الطبية تستدعي خبيرا طبيا في تخصصه، والذي يقف على قمة الهرم فيها الطبيب الشرعي صاحب المسئوليات الجسام في هذا الشأن ... بمعنى أن القاضي حين يقوم بالاستعانة بالخبرة، عندما يرى ضرورة لذلك، فإنه يسعى الى الخبير بحسب تخصصه. ومجال التخصص محكوم بقاعدة طبيعية وهي قاعدة العلم المؤسس على التحصيل الدوري الدراسي كما هو الشأن في دراسة الطب او الهندسة او العلوم الفنية في مجال الجريمة كدراسة علم البصمات وعلوم الصيدلة والتحاليل والاختصاص في مجال الكهرباء والالكترونات .... الخ. وهذه كلها أمور تحتاج الى دارسيها الذين انتهجوا دراسة المنهج.

وإذا كان القانون قد اخذ في الاعتبار ضرورة توافر الأركان الشكلية والموضوعية في الخبرة فإنه - وإمعانا في المحافظة على هذا الأمر - يقوم القضاء بالاستعانة بخبراء مصنفين في هذا الشأن مما هو مندرج في قائمة المحكمة، وهو ما يطلق عليه نظام جدول الخبراء الذي يتميز به النظام القانوني الفرانكوفوني، دون نظيره الأنجلوفوني، فحين يندب القاضي في هذا النظام خبيرا فإنه يقوم بذلك مستعينا بجدول الخبرة المعد في كل محكمة. على إن هذا الأمر غير مقيد للقاضي، وإنما يجوز للقاضي ندب خبير من خارج الجدول، وإن كان القضاء الفرنسي يستلزم في هذه الحالة ضرورة أن يقوم القاضي بتسبيب قراره هنا وإلا ترتب البطلان على قرار ندب الخبير[42]. أضف إن القانون يتطلب اجراءات شكلية أخرى في الخبير ينبغي توافرها كحلف الخبير اليمين ... الخ، وهذه كلها إجراءات يترتب على مخالفتها البطلان إن لم يقم الخبير بمراعاتها.

ولكن السؤال المطروح هنا يتمثل في مدى امكانية قيام القضاء باللجوء الى الخبرة حين اعتراض قضائه موضوعا من موضوعات الانترنت؟ سيما وهو يواجه قاعدة خطرة تتمثل في حداثة موضوع العالم الافتراضي او الرقمي ككل، مما يعني إن ما يمكن أن يردد كنتيجة للخبرة يمكن أن يكون غير ما سوف يتقرر مستقبلا، ناهيك عن كونه يمكن أن يكون مثار جدل في الفترة المعاصرة. على إن مثل هذا القول لا يعفي في الحقيقة القضاء من ضرورة الاستعانة بالخبرة التقنية بحسب ما هو متاح.

42 د. سليمان عبد المنعم – بطلان الإجراء الجنائي – دار الجامعة الجديدة للنشر – الإسكندرية 1999 ص. 182

إن الخبرة التقنية في مجال الانترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدارسة التي (رغم عدم وجود نص يقيد القضـاء بضـرورة الاسـتعانة بها تحديدا) . ينبغي التقرير بأن دراسـات الحاسـوب والانترنت لا ترتبط بمنهج دراسـي او بحثي معين او حتى مدة زمنية يقضـيها المرء دارسـا في الجامعات والمعاهد المتخصـصـة، وانما ترتبط بمهارات خاصـة وبموهبة اسـتعمال الحاسـوب والانترنت والتعامل مع تقنية المعلومات، إذ إن أمهر مبرمجي نظم التشـغيل حتى الآن مثل Bill Gates لم يكن تحصـيله العلمي يتجاوز المرحلة الثانوية، وذات الامر ينطبق على عتاة الهكرة ومخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعلم الثانوي والسنوات الجامعية الاولى في أحسن الأحوال.

ومن هذا المنطلق تتميز الخبرة في مجال تكنولوجيا المعلومات عن الخبرة في أي فرع آخر من الفروع التي يمكن أن تكون محلا للخبرة أمام القضاء.

على أن الأمر هنا يحتاج الى مزيد من التأمل القانوني، ذلك إن عدم التركيز على النواحي التي تجعل الخبرة مرتبطة بركنها الشكلي، من شهادات او مراحل علمية او منهجية معينة، ينطلق تحديدا من التطوير السريع الحادث في تكنولوجيا المعلومات. وهو تطور يجعل الخبير- حتى الملهم والمسـتلهم لقواعد هذا التطور السريع ذي الطبيعة الفجائية - في محل من يبدي رأيه الشخصي المستوحى من منطق فهمه للأمور حسبما توقف عندها علمه ودرايته في موضـوع ليس له حدود يقف عندها Limitless domain، وهو يبدي رأيه هذا أين؟ في بيئة قانونية صرفه.. المحكمة ... بما يعني إن رأي الخبير لن يكون حين عرضه على المحكمة سوى رأي غير دقيق قابل للدحض بكل سهولة[43].

إن المثال العلمي الذي يمكن تقريره هنا، إن الخبير التقليدي يملك وسـائله العلمية التي تسـاعده على إعداد تقرير يستند الى منطق علمي يساعد القاضـي في بناء او تحديد الواقعة لكي يحكم فيها بالبراءة او بالإدانة، فمثلا إن الخبير الحسابي يجري دراسته كخبير قضائي مثلما هو الحال حين يؤدي عملا آخرا، فهو يستخدم ذات الأسـاليب والمعادلات الرياضـية التي سـوف يسـتخدمها كخبير حسـابي أمام القضـاء، وكذلك الطبيب والمهندس.. الخ، فكل من هؤلاء كما إنه يكون دارسـا لمنهج تخصـصـه فإنه أيضـا تتكون لديه القناعة والثقة في المنهج الذي يعمل بمقتضاه باعتباره منهجا علميا يستند الى حقائق العلم. أضف الى ذلك أنه حال حدوث تطوير في منهج الخبرة التقليدية - تجاوزا - فإن هذا التطوير يتداركه جميع الخبراء في المجال المطلوب.

في حين أن خبير الحاسوب والانترنت يظل دائما في حالة شك قائمة في منهجه، سيما إذا اعتمد الدفاع في تشـكيك المحكمة في رأي الخبير على حقائق علمية جديدة، تجعل رأي الخبير عرضـة للهدم. إذ فضـلا عن أن الأمر لا يحتاج الى خبرة دارسـة في مجال الحاسـوب والانترنت، فإن التطور الحادث فيه يجعل من الصعوبة بمكان متابعته على النحو الذي يحقق الالمام التام والكلي بموضوع هذا الفرع من العلوم وهو فرع تكنولوجيا المعلومات. لذلك فإن متطلبات الخبرة من الناحية الشـكلية لن يكتب لها الاسـتمرار في إطار تكنولوجيا المعلومات، ومثل هذا الأمر ينبغي أن يدركه المشرع جيدا وإلا وقع تشريعه في خلل عدم التفاعل مع حقيقة وجوهر التعامل مع جرائم الحاسوب عامة، والانترنت على وجه التخصيص. فمثلا إن الصـراع بين مدى امكانية تحديد مسار الانترنت وعدمه يشكل صراعا جوهريا من حيث المبدأ، وإن كان الراجح هو

[43] **Ross Thomson, John Huntely, Val Belton, Fen Li & Jim Friel - The legal data refinery - P.1, International journal of law & technology, vol. 8 , issue 1, Oxford UNI. Press 2000.**

الاتجاه الى عدم امكانية تحديد مسـار الانترنت حتى مع امكانية تحديد هوية IP الحواسـيب وأماكن وجودها[44].

وإذا كان ذلك الذي سـلف كذلك فإن الامتداد الطبيعي للتسـاؤل المثار حول الخبير التقني يخرج عن إطار التحديد الفني- القانوني، الذي يعرفه القانون الاجرائي في صيغته التقليدية، ومن ثم- في رأينا- يمكن للقضاء الاستعانة بخبير غير دارس، بيد إنه يملك الخبرات اللازمة التي تمكن من التوصل الى الحقيقة. ويلزم لذلك السير بهذه القاعدة الى مطلق الاستعانة بها فيجب أيضا الخروج عن فكرة اعداد كادر متخصص او شركة متخصصة تعد خبيرا قضائيا يستعان به في كل الدعاوى التي تعرض على القضاء، كما هو الشأن في شركة AOL –قبل بيعها الى Time Warner- التي كانت تعتمدها المباحث الفيدرالية الامريكية كخبير لها. ذلك إنه في إطار تكنولوجيا المعلومات ومعالجتها الآلية ليس من السهولة الإقرار بوجود متخصص منفرد، حتى وإن كان يملك القدرات المالية على الظهور بمظهر المتفرد في مجال الخبرة القضائية. لذلك يسمح نظام الخبرة في ثوبه الجديد، بالاستعانة بشركات او منظمات او مؤسسات متخصصة بل والأفراد بقدر من الإنسيابية في تعاملاتها، فمثلا يجوز للشركة حين تكون من أعوان الخبرة القضائية، القيام بتوظيف أي كان والتعاقد معه لمدة او مدد معلومة او في إطار كل موضوع على حده، فيكون تقريره المقدم كما لو كان مقدما بأسم الشركة كخبير قضائي.

ويلزم هنا الإقرار بضرورة عدم الاعتراف بالخبرة التقنية كاستثناء على القاعدة الأصلية المقررة في القانون، وانما في رأينا إنه آن الأوان لإعادة النظر في قواعد الخبرة في الاجراءات الجنائية، بشكل يجعل هناك توافقا بين القاعدتين، وبحيث لا يكون هناك قاعدة أصلية وأخرى استثنائية وانما قاعدتان أصليتان. ذلك إن الخبير التقني لا يقوم باستجلاء حقيقة جريمة محددة، وانما في الواقع يقوم باستجلاء أشكال مختلفة من الجرائم. فليس الأمر مرتبطا فقط بجريمة سرقة عبر الانترنت او قرصنة على حقوق ملكية فكرية او تخريب معلوماتي او تعديل في نظم معلومات او ... الخ، وانما أبعد من ذلك فهو يتفاعل مع بيئة متعددة الاستخدامات هي الانترنت، وهذا يستلزم بالطبيعة أن يكون على دراية بالحاسوب ونظمه. بل وأبعد من ذلك إن إصدار قاضي الموضوع لقرار تعيين خبير قد يلزمه التعرض لبحث مدى امكانية تعيين أكثر من خبير في الدعوى المنظورة أمامه، لصعوبة مهمة الخبرة التقنية في الغالب من الأحوال، وهو ما نتعرض له في الفقرة القادمة.

- قاعدة تعدد الخبراء: - يعترف التشريع المقارن بقاعدة تعدد الخبراء في الدعوى الواحدة، بحيث يمكن أن يكون لكل منهم دورا محددا من ناحية. ومن ناحية أخرى فإن التشريع الإجرائي على الرغم من إن سير ونمطية العمل بمقتضاه استلزمت ضرورة أن يكون الخبير شخصا طبيعيا، فإنه لم يتقرر بالنص لزوم ذلك، وانما أطلق المشرع للقاضي الجنائي امكانية الاستعانة بالخبير، الذي من الممكن أن يكون شخصا طبيعيا كما من الممكن أن يكون شخصا معنويا كمؤسسة متخصصة تعمل في مجال الخبرة التقنية.

أضف ان المشرع الجنائي لم يقرر ضرورة أن يكون في الدعوى خبيرا واحدا فقط، وانما منح القاضي الجنائي صلاحية ندب أكثر من خبير في الدعوى. ومثل هذه النصوص[45] تتجاوب مع الحال الذي عليه

---

[44] – د . جميل عبد الباقي الصغير – الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – المرجع السابق ص. 44 ، وراجع أيضا
- Valerie Sedallian, Droit de L'internet op – cit P. 132.

[45] القانون الليبي في مواد الخبرة (14 – 59 – 265 – 266 – 319 – 516).

الخبرة التقنية، سيما وإن مجال تكنولوجيا المعلومات يثير جدلا متواصلا حول مقدمات التعامل معه، وكذلك النتائج الممكن تحقيقها فيه. ومن ثم يلزم أن يكون في الدعوى أكثر من خبير، حتى إنه يمكن القول إن الأصل في الخبرة التقنية هو تعدد الخبراء، بحيث يجب ألا يكون هناك خبير واحد في الدعاوى التي يكون موضوعها الانترنت والحاسوب.

المبحث الأول
أنواع الخبرة التقنية

إن الخبرة التقنية في مجال المساعدة القضائية تعد أقوى مظاهر التعامل او التفاعل القانوني / القضائي مع ظاهرة تكنولوجيا المعلومات / الانترنت، ذلك إنها تؤدي دورا لا يستهان به إزاء نقص المعرفة القضائية / الشخصية لظاهرة الانترنت. وهذا أمر لا يعني سوى إن القضاء يتعامل مع الواقع في صورته التقليدية كما المتطورة من ناحية، كما إن ذلك يعني من ناحية اخرى إن الظواهر الجديدة حتى وإن تدخل القانون لوضع حلول للمشاكل التي تطرحها فإن الدور القضائي في تفسير هذه النصوص القانونية يظل دورا أصليا في هذا الإطار، وهو لكي يؤدي دوره يلزمه الاتفاق مع طبيعة التقنية بعيدا عن الافتراض. وهنا يأتي دور الخبرة التقنية في مجال الانترنت من حيث كونها أداة رئيسية لتكوين الحكم القانوني / الجنائي سواء في النظم الانجلوفونية او في النظم الفرنكوفونية.

ولكن كيف يمكن التعرف على الخبرة التقنية؟ وما هي أركانها؟ وهل تختلف - بالتالي - عن الخبرة كما يعرفها النظام القضائي؟ ومثل هذا التساؤل الاخير سوف يقودنا حتما الى التطرق الى الشروط الضرورية التي يلزم توافرها في الخبير لكي يمكن لعمله أن تتكامل أركانه أمام القاضي.

أولاً - الخبرة التقنية وتصنيف الحصول عليها: - في إطار مسألة طرح فكرة كيفية الحصول على الخبرة التقنية طرح **المرشد الفيدرالي الامريكي للبحث والتقصي في الحاسوب**، الذي ضم في جنباته خبرات أكاديمية للتعامل القانوني الإجرائي مع الحاسوب وتقنيته أفكار جوهرية تتعلق بتصنيف التعامل مع الخبرة التقنية، كان أبرز ما فيه تصنيف كيفية الاستعانة بالخبرة.

ولقد كان في مقدمة التصنيف هو اللجوء الى الخبرة الفيدرالية وهي تلك التي تتبع منظمات العمل الحكومي للاتحاد الفيدرالي، والتي عددها في الملحق الثالث من المرشد، ثم تطرق بعد ذلك الى المنظمات الأخرى غير الحكومية التي يمكن اللجوء إليها في هذا المجال حال عدم وجود خبراء انترنت لدى الجهات الحكومية يمكن للجهات القضائية الاستعانة بها.

على أن هذا الطرح الامريكي في الحقيقة يجعلنا أمام فرضين، إما أن يفتح المشرّع المجال لامكانية الاستعانة بالخبير الأجنبي، لكي يمكن أن يكون محل عرض وطلب من قبل الدول التي ليس لديها الكفاءة في مجال تكنولوجيا المعلومات / الانترنت. وإما أن يكون هذا الحل ليس من متطلبات المرحلة المعاصرة بالنسبة لهذه الدول، وهو الأمر الذي يتعارض حتى مع فكرة الإعداد المسبق لخبير الحاسوب والانترنت. وهي الفكرة التي طرحها المرشد الفيدرالي المذكور الذي قرر **ضرورة توافر الخبير قبل الواقعة الإجرامية**[46]. وهو مبدأ يجعل عملية السعي الى البحث المتواصل على الخبرات بقصد ضمها إلى الثقافة

[46] **"The trick, of course , is to find the expert while planning for the search and not to start looking after the agents excute the warrant ". Federal guidelines for searching and seizing computer . IV , I , 2 / a . availble online in dec. 2000 at :**

المنظمة التي تنتهجها الدول في إطار الانترنت ذات الأسبقية في هذا الشأن. وبما يجعل أيضا عملية حركة تصدير واستيراد القدرات التقنية هنا ذات علاقة بتطوير هذا المجال التقني[47].

والحقيقة إن كلا من الحلين السالفين من الحلول التي تصنع مفارقة ليس لها منطق التعامل مع الأحداث، وإذا كان المرشد الفيدرالي الامريكي المذكور يعد مرشدا غير ملزم من الأساس، وإنما هو مجموعة توجيهات، فإن الاتجاه الذي سلكه يضع الباحث في فرضية احترام التعامل الحكومي أولا، ومثل هذا الفرض يخرج عن المبادئ الأساسية التي يعرفها النظام القضائي الانجلوفوني الذي لا يعترف بوجود فكرة جداول الخبرة القضائية في المحاكم كما هو مقرر في النظم القضائية التي تتبع الاتجاه الفرانكوفوني.
كما أن القضاء المصري يتجه الى ضرورة لجوء قاضي الموضوع الى جداول الخبرة القضائية المعتمدة في المحكمة وإذا ارتأى غير ذلك عليه تسبيب قراره.

والاستعانة بجداول الخبراء في المحكمة تعد في إطار النظم الانجلوفونونية فكرة جديدة بدأ يتقبلها كنوع من التجديد، تحت وطأة الاتجاه الذي برز في ظل ثورة المعلومات من أجل ضم الخبراء في هذا المجال الجديد تحت مظلة العمل الحكومي. وهذا الاتجاه سوف يكتب له النجاح حقا في ظل النظام الانجلوفوني من حيث الهيكلة الإدارية، إلا إنه من الناحية الموضوعية سوف يستقر عند المشكلات التي تفرضها الخصوصية التي عليها تكنولوجيا المعلومات / الانترنت، ومثل هذا الامر سوف يجعل الخبرة التقنية / الانترنت على ذات المنوال التي هى عليه من مشاكل سيما في إطار موضوع تصنيف الخبرة هنا.

ثانياً ـ المشكلات القانونية الجديدة: ولعل أعتى المشاكل التي سوف تواجه نظم الخبرة عامة تتمثل في تكوين الخبير الذي سوف يتم الاستعانة به، ذلك ان الاستعانة بالخبرة في مجال تكنولوجيا المعلومات / الانترنت لا يعتمد على شهادة خبير تتوافر فيه الشروط الشكلية والموضوعية التقليدية المتطلبة في الخبير، وإنما خرجت تكنولوجيا المعلومات / الانترنت هنا عن ذلك. فما هو متطلب في الخبير من عناصر شكلية ، كما هو الشأن في التخصص باكتساب المعرفة من خلال دراسته وحصوله على شهادات من مؤسسات تعليمية ، قد يصلح أن يكون محل دفع أمام محكمة الموضوع ، وقد يكون من الدفوع الموضوعية الجوهرية أيضا في هذا الاطار ، وقد يصلح أن يرتقي الى أن يكون دفعا من طبيعة قانونية لكونه يلتحم بحقوق الدفاع أيضا ، إلا إنه مع ذلك لن يكون له ذلك التأثير في اطار تكنولوجيا المعلومات / الانترنت التي تتعاطى منطلق التعامل التقني مع الانترنت من خلال النهوض بالفكرة الموضوعية دون تلك الشكلية في هذا الاطار ، فما هو مقرر في اطار تكنولوجيا المعلومات انما يرتبط بفكرة التعامل مع الانترنت من زاوية القدرات التي ينجبها الطابع التقني الخيالي ، إذ ان اغلب الجرائم التي ترتكب عبر الانترنت إنما يرتكبها أشخاص لم يكونوا قد تجاوزوا مرحلة التعليم الثانوي، وفي الأقل القليل كان مرتكبوها من المتخصصين، بل إن سابقة البرمجة التاريخية التي أرساها بيل جيتس وبول الن وهما لم يتجاوزا مرحلة التعليم الثانوي لتعد سابقة تاريخية يلزم أن تؤخذ في الاعتبار من هذه الزاوية، فالنجاح الاقتصادي كان حليفهما في حين انتهى تيم بيرنرز لي مخترع شبكة المعلومات الدولية www كمدير فني في معهد ماساشوستس للتكنولوجيا يتقاضى راتبا متوسطا .
والحقيقة التي لا يمكن أن تكون محلا لجدل تصنيفي أن الاتجاهات المقارنة في موضوع الخبرة القضائية يتنازعها رياح التغيير في منطق التعامل مع الخبير الذي يؤخذ من رأيه دليل على تقييم منطق الجريمة من حيث كيفية وقوعها ، فمن ناحية إن النظم الانجلوفونية لتجد في منطق او قاعدة الضم والاحتواء التي

---

http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm

47 وللأسف ترى الدول النامية ان ذلك في مصلحتها حيث انها اشترطت للدخول في اتفاقية الجات ان تكون هجرة العقول مما يدخل في إطار تجارة الخدمات.

تضعها في سبيل احتواء القدرات التقنية أساسا تنطلق منه لتضم بين جانبي هذه القاعدة الخبراء في مجال تكنولوجيا المعلومات / الانترنت، ومن ثم تلجأ الان الى الاستعانة بنظام الخبراء المقيدين في جداول المحاكم كتطبيق له سابقة في التشريع المقارن ، في حين إن الاتجاهات الفرانكوفونية لتجد ذاتها في ذات المأزق بشكل آخر ، إذ لا يكفي ما لديها من قدرات خبراتية حكومية يمكن للقضاء الاستعانة بها في وضع الحلول الفنية والتقنية في مجال الانترنت من ناحية أخرى.

ومن هذا الأمر ليجعل موضوع منهج التعامل مع الخبرة التقنية غير موحد، فما يصلح في دولة او مجتمع معين قد لا يكون نافعا في دولة او مجتمع آخر. ومثل هذا الأمر سوف يطرح العديد من المشكلات على المستوى الدولي حين الشروع في اعداد اتفاقيات تعاون قضائي في مجال تكنولوجيا المعلومات / الانترنت.

ثالثاً ـ التصنيف المقترح لأنواع الخبرة في الانترنت: ـ إن الاعتماد على الأسلوب الحكومي للتعامل مع ظاهرة الانترنت، سيما في إطار نظم الإثبات، ليجعل من منطق المفاضلة والتبعية هو المنطق السائد. ومثل هذا الامر سوف يجعل الجريمة تتفوق على العدالة وأجهزتها في شكل يؤدي دون شك الى سيادة منطق الجريمة.

وإزاء هذه النتيجة فلا يسعنا إلا التقدم - في اتجاه اخر نقترحه هنا - لوضع تصنيف يمكن المساعدة في احداث توازن بين التطور الامريكي حسبما هو مقرر في المرشد الفيدرالي المذكور وبين المعطيات الموجودة في الدول الأخرى - سيما ذات النمو البطيء هنا. وهذا التصنيف المقترح نعرضه على النحو التالي:

أ: **الخبرة الخاصة: ـ** وهذه تعد أقوى أنواع الخبرة على الاطلاق لكونها تنطلق من مفهوم السعي الى خلق فرص منافسة حقيقية بين المنظمات الخاصة.

ويبدو أنه من اللازم وضع تعريف للخبرة الخاصة بحيث تضم في جنباتها الخبرة الفردية ايضا لكونها من وجهة نظرنا تعد أقوى مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات / الانترنت، ويكفي هنا أن نذكر إن المؤسسات الكبرى المتخصصة في الحاسوب والانترنت لتسعى بكل جهودها الى الاستعانة العقدية بأشخاص اثبتوا كفاءتهم في مجال الحاسوب الانترنت. حتى عصاة القانون منهم فإن اتجاه اقتصادي يحاول إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون، وانما يلزم اللجوء الى الحلول الاقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الاقتصادية، بل إن من الدول ما يسعى جاهدا الى محاولة التعرف على هكرة تحولوا مع مرور الوقت الى رموز وطنية جراء تحركاتهم عبر الانترنت.

والى جوار الأفراد توجد المنظمات الخاصة في كافة المجالات والتي سوف يكون لها السبق في مجال الخبرة، فالقضاء الفرنسي في قضية اتحاد الطلبة اليهود الفرنسي ومنظمة ليكرا ضد شركة ياهو استعان بخبراء من خارج الجدول وتحديدا من القطاع الخاص في خارج فرنسا في هذا المجال لكي يضعوا رأيا فنيا يتعلق بامكانية الفلترة والتصفية عبر الانترنت.

وتختلف المنظمات الخاصة ما بين منظمات أهلية تتصدى لكل محاولة من المجرمين بقصد التعدي على الحقوق الالكترونية، وبين نوعية من المنظمات تسعى الى فك طلاسم العالم الافتراضي على أسس تجارية. فقد استطاعت إحدى الشركات الأسكتلندية المتخصصة في برمجيات الحاسوب والانترنت هي Scottish Software Co. من إعداد مشروع خريطة للعالم الافتراضي على غرار الخريطة الجينية للإنسان The

Human Genome، ولقد قام بإعدادها مجموعة من خبراء البرمجية الأسكتلنديين كانوا قد شرعوا في إعداد هذا العمل في عام 1998 واستغرق إعدادها ثمانية عشر شهرا.

ولقد كان من أهم نتائج هذه الخريطة أن تمكنت الخبرة الخاصة من رصد حركة الجريمة عبر الانترنت، ومعرفة تطوراتها في كافة مظاهرها وأشكالها، حيث برز أكثر من أربعين مظهرا من مظاهر الاجرام عبر الانترنت. ولقد أمكن من خلال ما تم رصده في إطار خريطة الجريمة عبر الانترنت أن أدرك الخبراء وجود ما يربو عن المائتي ألف موقع جديد للدعارة عبر الانترنت، ولقد استفاد أهل الخبرة الخاصة من رصد هذه الخريطة في التعرف على التهديدات الحقيقية التي تواجه الدول والأفراد، فمثلا فن إخفاء النصوص بإضافة نصوص اخرى Steganography يعد من أخطر المشاكل التي تواجه العالم الافتراضي / الانترنت فمثل هذه المشكلة تعد ثالث أخطر مشكلة تواجه النظام الأمني في الولايات المتحدة بعد العدوان البيولوجي والكيمائي[48].

ب: المؤسسات التعليمية: - لما كانت الانترنت تعد أحد منتجات العلم في حركته (التقنية)، فإنه يمكن القول وبحق إن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات التعليمية. فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل، وفي مجال دراستنا تقدم خبراء مدعومون بالمنهج.

وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية، كما إن التفكير العلمي لا يمكن تجنبه في رصده للظاهرة الانسانية. والاتجاه العالمي في رصد تطورات الجريمة عبر الانترنت يتجه الى المؤسسات العلمية بحيث يتم دعمها ماديا ومعنويا، لتكون أفضل سبل المواجهة، سيما وإن المعتقد السائد في مواجهة الجريمة ينطلق من الوسائل التي من ذات طبيعة السلوك الإجرامي، فكما أنه ليس هناك أفضل من الأطباء لسبر غور الجريمة الطبية، والماليين لسبر غور الجريمة المالية والنقدية ... الخ، فإنه ليس هناك أفضل من التقنيين في المعلوماتية لسبر غور الجريمة عبر الانترنت.

ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهبة الاستعداد لمواجهة الجريمة عبر الانترنت، ومن ذلك دراسات الحاسوب التي تتطور بشكل فائق في جامعة ستانفورد، كذلك معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق.

ومن التشريعات التي اعتمدت المؤسسات التعليمية كبيت خبرة في المواد الجنائية التشريع الفلسطيني، فقد نص قرار رئيس السلطة التنفيذية لمنظمة التحرير الفلسطينية / رئيس السلطة الفلسطينية رقم 16 / 1998 المؤرخ 20 / 3 / 1998 [49] في المادة الأولى منه ، على **"إن التقارير الصادرة عن مختبرات جامعة القدس او النجاح او بير زيت او الأزهر او الإسلامية والموقعة بتوقيع الموظفين المسئولين عنها والمتضمنة نتائج الفحص الكيماوي او التحليل الذي أجروه بأنفسهم بشأن أية مادة مشتبه بها ، تقبل في معرض البينة في الإجراءات الجنائية كأنها صادرة عن مختبر الحكومة الكيماوي او من محلل الحكومة**

---

48 Marcus Gibson – Infowar, Financial Times Oct.20, 2OOO. available online in oct.2000 at: http://www.infowar.com/ccr/ccr1.shtml

49 الوقائع الفلسطينية – السنة الخامسة . العدد الثالث والعشرين في 8 / 6 / 1998 – موسوعة التشريعات العربية (الاستاذ محمد ابوبكر بن يونس) ، فلسطين / باب إجراءات جنائية .

الكيماوي". وإن كان المشرّع الفلسطيني يحتاج الى توسعة نطاق نفاذ هذا التشريع بحيث يتم تعميم الخبرة الى أبعد من مجرد التحليل الكيماوي، وبما يجعل للمؤسسات التعليمية مساحة خبرة تتناول كل الامور بما في ذلك تكنولوجيا المعلومات.

ج : جهات الضبط القضائي: - أشرنا فيما سبق الى موضوع ضرورة التخصص في مجال الضبط القضائي، وهنا نجد لزاما علينا التعرض الى نشاط الدول في اعداد أجهزة متخصصة للخبرة في الإجرام عبر الانترنت. وهو نشاط – في الحقيقة - تتزعم الولايات المتحدة فيه قائمة أجهزة الضبط القضائي في العالم، بحيث تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الانتربول أيضا. وكان آخر نشاط مؤسسي في هذا الاطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الامريكية FBI أطلق عليه **المعمل الاقليمي الشرعي للحاسوب**[50] ، ومقره سان دييجو San Diego ، والذي تم افتتاحه في نوفمبر 2000 لكي يكون بيت خبرة عام متعدد النواحي القضائية غرضه مكافحة التصعيد الخطير في الجريمة عبر الانترنت ، وذلك بتحليل وتصنيف الدليل الرقمي بحيث يتم اعداد محللين شرعيين للحاسوب Computer forensics examiners الذين سوف يكون لهم أهمية كبرى في نطاق العمل على تكثيف مواجهة الجريمة عبر الانترنت - كما يقول مدير الـــ ... FBI (السابق) لويس فريح Louis J. Freeh -. ويبرز تعدد النواحي التي يتعامل معها المعمل الشرعي الجديد كونه يتكوّن من التقاء العديد من منظمات الضبط القضائي تتعاون فيما بينها لكي يحقق الفائدة المرجوة منه، مثل إدارة مكافحة المخدرات Drug enforcement administration، ووحدة التحقيقات لمكافحة المجرمين Defense criminal investigative services، ووحدة تحقيقات الجريمة في البحرية Naval criminal investigative services، ووحدة الجمارك US customs services ومكتب النائب العام للمقاطعة ومكتب حاكم المقاطعة وإدارة شرطة كاليفورنيا.

ويوجد بالمعمل المذكور ثلاثة فروع الأول هو Imaging والثاني Analysis والثالث Research and development، وبحيث يكون تدريب الخبراء فيه بشكل دائرة متكاملة وبحيث يقوم تدريبهم على الفروع الثلاثة [51].

د: دور المجني عليه: - إذا كانت الاتجاهات الحديثة في القانون الجنائي تبنى على دراسات تتعلق بالبحث في دور المجني عليه من الجريمة في الجريمة ذاتها، فإن مثل هذا الاتجاه يجد مغزاه عبر الانترنت في ذلك المنعطف السلبي في دور المجني عليه في مكافحة الاجرام عبر الانترنت. حيث ان المجني عليه في هذه النوعية من الجرائم كثيرا ما يلجأ الى اتخاذ دور سلبي حماية لمصالحه التي تتعلق بصفة خاصة بسمعته إذا كان له صفة تجارية كما لو كان مصرفا او محلا تجاريا، أضف الى ذلك ان المجني عليه إذا كان شخصا طبيعيا في دولة لم تتخذ الخطوات الجادة نحو تقنين الانترنت والحاسوب عامة فإن سلوك الضبط القضائي فيها قد يجعل من المستحيل إقامة ذلك التوازن بين نظام العدالة الجنائية وبين المجني عليه. ومثل هذا الأمر ينتهي غالبا الى الأخذ في الاعتبار نوعية خاصة من المجني عليه في جرائم الانترنت كما هو الشأن في بعض منظمات الدولة ومؤسساتها، وكذلك فيما يتعلق بالأشخاص الطبيعيين كما هو الشأن في الأحداث وصغار السن حيث يتولى القانون فرض حماية جنائية مشددة عليهم عبر الانترنت.

---

[50] **The regional computer forensics laboratory**

[51] **Jerry Seper – FBI steps up efforts to fight crimes related to computers, the Washington times, available on line in nov. 2000 at: http://www.infowar.com**

ولقد كان موضـوع المجني عليه عبر الانترنت من الموضـوعات الدقيقة التي أفسـحت المجال بشـكل كبير لموضـوع التعاون الدولي في مكافحة الإجرام عبر الانترنت، وصـولا الى ضـبط الجناة في هذه النوعية من الجرائم. سيما وان الانترنت أفسحت المجال لتعامل صـغار السن بها وبشـكل اتضـح فيه أهمية دورهم لما يتمتعون به من خيال خصـب وسـعة أفق يحتاج الى العمل في الانترنت. لذلك لا نجد هناك مانعا من التقرير بأهمية دور المجني عليه الصـغير او الحدث في الدخول معترك الخبرة هنا، خاصـة في النواحي الفنية حيث ان هذه النوعية من المجني عليهم يمثلون المستقبل بالضرورة، وعلماء التقنية متفقون على ان الانترنت هي تقنية المستقبل. فالمسألة فيها توازن كبير من هذه الزاوية.

هـــ : التعاون الدولي: - وقد يكون مفيدا في هذا الإطار التعرض لمنطق التعاون الدولي في مجال الخبرة التقنية. والحقيقة أن مجال التعاون الدولي انما يعد تقريرا مسـبقا بأهمية اللجوء الى المنظمات الحكومية في الإطار الاقليمي، إذ يستلزم التعاون الدولي أن يكون بين حكومات معترف بها في هذا الشأن، وفي هذا تقوية للاتجاه الوظيفي كما أسـلفنا. في حين إن السـؤال في مجال تكنولوجيا المعلومات ينطلق من مدلول مدى إمكانية أن يكون هناك تعاون دولي في مجال منطق التعاون القضـائي وتسـليم المجرمين، حتى وإن كان هؤلاء من العاملين في حقول فنية تتعلق باقتصاديات ودعم اقتصاديات الدول.

ولقد كان المؤمل من اتفاقيات دولية في مجال مكافحة الجريمة عبر الانترنت أن ينص فيه على أفكار جديدة تسـمح بقدر من المعقولية من حيث الأخذ في الاعتبار الحصـانة التي تمنحها بعض الدول لهكرة يعملون في حقول مشروعة، ثم انهم يرتكبون جرائم وأعمالا غير مشروعة بما يفرض عليهم نوعا من الحصـانة التقنية ذات المغزى السياسي في هذا المجال.

المبحث الثالث
عمل الخبير التقني

ينعقد الاختصـــاص للخبير التقني في أحد شـــكلين: إما أن يكون مكلفا بذلك من قبل احدى جهات التحقيق (الاصلية - الاستثنائية)، وإما ان يقوم بعمله بناء على أمر من محكمة الموضوع، وفي الحالين يعد الأمر الصـادر اليه قضـائيا. فإذا لم تتوافر الصـفة القضـائية للأمر الصـادر الى الخبير فإن ما ينتج من دليل عند عمل الخبير يعد دليلا غير مشـروع ومن ثم يحق لمحكمة الموضـوع ألا تأخذ به. فإذا حدث وأخذت به كان ذلك منها سببا كافيا لكي يتعرض حكمها هذا للنقض.

وهناك حالة ثالثة يمكن أن تضـــاف إلى الحالتين المشـــار إليهما وهي التي يشـــير إليها القانون كحق للمتهم (فقط) في الاستعانة بخبير استشـاري[52] ، حيث يجوز له استخدامه وقتما يشـاء أثناء التحقيق، ودون تحديد لمدة زمنية يلزم خلالها القيام بهذا الإجراء، وإن كان البعض يتجه الى ضـــرورة أن تكون اســـتعانة المتهم بالخبير الاسـتشـاري أثناء التحقيق[53]. وليس من سـند لهذا الرأي سـوى إن المشـرع وضـع النص الخاص بالخبير الاستشـاري كحق جوهري من حقوق الدفاع في الباب الخاص بالتحقيق الابتدائي. وعندنا إن المتهم يمكنه استخدام هذا الحق في أية مرحلة من مراحل التقاضي، وكذلك يمكن أن يستخدم هذا الحق حتى ولو لم يكن هناك وجه لإقامة الدعوى او تم حفظها بحيث يمكنه إضافة تقرير الخبير الاستشاري الى ملف الدعوى التي صدر فيها أمر النيابة العامة بالا وجه لإقامة الدعوى. وذلك استنادا الى ان موضوع الخبير الاستشاري يظل من حقوق الدفاع الجوهرية التي يملكها المتهم في هذا الإطار، والتي لا يجوز حرمانه منها وإلا عد ذلك سببا يبطل التحقيق ككل، كل ذلك مشروط بالطبع بألا يكون في الاستعانة بالخبير الاستشاري تعطيلا في سـير الدعوى، إذا كانت الدعوى في حالة حركة[54] . ويجب هنا التقرير بالدور الكبير الذي يمكن للخبير الاستشاري أن يقوم به في إطار جرائم الانترنت، خاصة في الوضعية المعاصرة التي تستلزم بالضرورة تطوير الخبرة القضـائية عموما، وهي خبرة تحتاج الى الكثير من الجهد من قبل مؤسـسـات الدولة القائمة عليها لتطويرها بما يجعلها تقوم بدورها المطلوب منها في هذا المجال.

وتتحدد حركة الخبير التقني عبر الانترنت في سـلوك سـبيل تحري الحقيقة من منطلق التفاعل الكامل مع منطق الانترنت كعالم رقمي له وجود متكامل قام البشـر ببنائه. وفي هذا الإطار يلزم الخبير التقني أن يكون ملما ليس فقط بتحديد منطق وقوع الجريمة وكيفية حدوثها وانما أيضـــا يكون له دور كبير في التعامل مع ادلة الرقمية التي يتم الحصـول عليها من خلال قيامه بدوره هنا. كل ذلك سوف نعرض له ببعض التفصـيل في الفقرات القادمة.

أولا - تحري الحقيقة: - إن قاضي موضوع حين يستعين بالخبير انما يلجأ هذا الملجأ سدا لذريعة التشكيك في الادانة، ومن باب أولى حين تكون الخبرة متطلبة سـيما في النواحي الفنية التي تحتاج الى تخصـص، بحيث يكون اسـتجلاء موضـوع الجريمة من الأهمية بمكان لتحديد مقوماتها والنتائج التي ترتبت على

---

[52] د. مأمون سلامة – الإجراءات الجنائية في التشريع الليبي – الطبعة الثانية – الجزء الاول، منشورات مكتبة الجامعة – الزاوية، ليبيا 2000 ص. 608

[53] المرجع السابق.

[54] تنص المادة (88 – أ. ج مصري) على انه " للمتهم أن يستعين بخبير أستشاري ويطلب تمكينه من الاطلاع على الاوراق وسائر ما سبق تقديمه للخبير المعين من قبل القاضي على ألا يترتب على ذلك تأخير في السير في الدعوى " وهو ذات النص في المادة (73 – أ. ج ليبي) .

ارتكابها في نتائجها. لذلك نلاحظ إن تقارير الخبرة تُعد من مقومات الحكم الجنائي في كثير من الموضوعات سيما في الجرائم ذات الطابع التقليدي كالقتل والسرقة ... الخ.

وفي إطار الجرائم الحديثة التي تأخذ بذاتها الطابع التقني فإن مثل هذه الجرائم تكون فيها الخبرة عنصرا رئيسيا، بحيث يتطلب الأمر ليس مجرد التعرف على الجزئيات التي تسمح بالإدانة، وبالتالي تحديد كيفية ارتكاب الجريمة من زاوية تقنية، وانما يكون قصد الخبير التقني أيضا التعرف على ما يمكن أن يكون فكرة تقنية جديدة تفيد القضاء ومدى إمكانية قبولها في القانون. وهو الاتجاه الذي سلكته محكمة باريس في قضية اتحاد الطلبة اليهود وليكرا ضد ياهوو حيث كان مطلب المحكمة حين استعانت بخبراء الانترنت التعرف على امكانية تحديد مسار أمني وذلك باستخدام الفلترة.

وإذا كان للقضاء مطلق الصلاحية في تحديد عمل الخبير طالما إن القصد هو التوصل الى الحقيقة كاملة ، فإن الاستعانة القضائية بعمل الخبير تتطلب أن يقوم قاضي الموضوع بتحديد الفكرة مسبقا للخبير تاركا إياه اختيار الطريقة المثلى في تحري هذه الفكرة توصلا الى نتائجها ، شريطة ألا يكون القضاء معدا العدة للإدانة كما حدث في قضية ياهوو السالفة ، حيث كانت المؤشرات توحي بضرورة الإدانة في هذا الشأن ، وهو ما يستدعي القول هنا إن ذلك يجعل حكم القاضي فيه عدم حيدة في هذا الشأن ، ومن ثم يجب أن يكون تحري الحقيقة عن طريق الخبرة مقصودا منه التوصل الى الادراك الفني المستعصي على القاضي حله ، وبحيث لا يكون هناك إيحاء من القضاء في ضرورة الإدانة.
والحقيقة أن مؤشرا في عمل الخبير التقني يوحي بوجود تطور على درجة من الخطورة هنا ممثلا مدى استجابة القضاء لعمل الخبير التقني على النحو الذي يحقق استفاضة في فهم عمل الانترنت، وعلى النحو الذي يجعل الخبير موجها للقاضي، سيما ازاء عدم وجود قواعد تشكل مقياس عام يعتمد عليه في تقنية الانترنت يمكن إدراكها بالعلم العام الذي يملكه كل شخص؟ ومثل هذا الأمر يخشاه علماء القانون وترددت فيه الآراء بحيث يمكن القول، على الرغم من وجود أنصار بين اتجاه و آخر، إنه من الصعوبة بمكان اللجوء الى الخبير قصد الحصول على نتائج توجيهية لقاضي الموضوع، بل أن مثل هذا الأمر إن حدث يضع الخبير فعلا في مرتبة قاضي الدعوى وهو الأمر الذي – إن لم يكن قد عزل دور القاضي الجنائي - فإنه يجعل للدعوى قاضيا آخر غير مرئي.

وتحري الحقيقة يتخذ له مكانا كبيرا في سير عمل الخبير لكي تستطيع سلطات التحقيق والاتهام الرد على دفوع قد يبديها مرتكب الجريمة وتُشكّل في ذاتها دفوعا مقبولة أمام القضاء ، لكونها تتفق من حيث طبيعتها مع تكنولوجيا المعلومات والمدى الواسع التي هي عليه ، ومن ذلك الدفع الذي يبديه المتهم بكون ما تم ضبطه في حاسوبه ليس له به علاقة ولا يدري عنه شيئا ، وانما من قام بذلك هو أحد الهكرة مثلا او أن يكون ذلك هو مأمور الضبط القضائي ذاته لأي سبب كان[55]، ومعلوم ان انتهاك حاسوب الغير من الأمور الجائزة الحدوث في جرائم الانترنت ، فمثل هذا الأمر يحتاج بالضرورة الى الخبير للرد عليه، سيما وانه دفاع مقبول أمام المحاكم في القانون المقارن [56] . فلا يجوز للمحاكم إنكار مثل هذا الدفع عن المتهم ، لكونه دفعا جوهريا واقعيا يحتاج للرد عليه من قبل محكمة الموضوع وإلا وقعت في محظور الخطأ في التسبيب.

وإذا كان الأمر على ما سلف، فما هي أذن أساليب الخبير التقني في تحري الحقيقة سيما إذا كان بصدد مسألة من المسائل الجديدة على العمل والتقنية، مثلما هو الحال في تكنولوجيا المعالجة الآلية للمعلومات / الانترنت؟ هذا ما نعالجه في الفقرة القادمة.

---

[55] **US v. Gregory James Grant , No. 99 – 2332 , July 17 , 2000 . op cit**

[56] **USA v. Hay, App 9th Cir. No. 99 – 30101, 24 Oct. 2000. Op cit**

ثانيا - أســـاليب عمل الخبير التقني: - للخبير التقني في ســـبيل تحري الحقيقة ان يقوم بكل ما يمكنه من التوصـل اليها. وهو في إطار القيام بعمله ان يسـتخدم الأسـاليب العلمية التي يقوم عليها تخصـصـه وليس للمحكمة ان ترفض تلك الأساليب ما يكون رفضها لها مسببا بشكل منطقي والا تعرض حكمها للنقض.

وهناك أسلوبان لعمل الخبير التقني:

الأول: - القيام بتجميع وتحصـيل لمجموعة المواقع التي تشـكل جريمة في ذاتها، كما هو الشـأن في التهديد Intimidation او النصـب Fraud او السـب Defamation او جرائم النسـخ Infringement of copyrights وبث صـور فاضـحة بقصـد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق الابيض ودعارة الأطفال وغيرها. ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسـبتها الى مسـارها الذي أُعدت فيه، وتحديد عناصـر حركتها، وكيف تم التوصـل الى معرفتها، ومن ثم التوصـل في النهاية الى معرفة بروتوكول الانترنت IP الذي ينسب الى جهاز الحاسوب الذي صدر عنه هذه المواقع.

الثاني: - القيام بتجميع وتحصـيل لمجموعة المواقع التي لا يشـكل موضـوعها جريمة في ذاته، وانما تؤدي حال تتبع موضـــوعها الى قيام الافراد بارتكاب جرائم. كما هو الحال في المواقع التي تســـاعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناســـب وزن الانســـان بادعاء أنه إذا تم تتبع التعليمات الواردة فيها فلن يصـاب الشـخص بحالة إدمان، وأيضـا كيفية زراعة المخدرات بعيدا عن أعين الغير (ويطلق عليه في هذه الحالة الفضـــولي) وأيضـــا كيفية أعداد القنابل وتخزينها ، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها[57]، وكذلك القيام بتحديد مسـار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت ، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشـــتركا لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج الى الانترنت من محل أقامته[58]، وهذا الأخير من الدفوع التي تلتزم محكمة الموضوع بالرد عليها.

ويتم في إطار تصـنيف المواقع المذكورة اسـتخدام برمجيات متطورة مهمتها الكشـف عن مثل هذه المواقع باستمرار، ومعرفة الجديد فيها. ثم إن هذه البرمجيات تتطور باستمرار حيث إن إمكانيات تصميم الصفحات عبر الانترنت تتطور بشـــكل ملحوظ بحيث يمكن القول إنه وإن كانت توجد معايير متفق عليها في اعداد الصفحات والمواقع إلا إن تفاصيل هذه المعايير هى التي تتطور بشكل مستمر.

الثالث - التحفظ على الأدلة: - التحفظ على الأدلة من العمليات الروتينية التي يلزمها الدقة دائما، والتي تباشرها جهات الاستدلال والتحقيق توصلا الى رصد قيمتها فيما يعرف في القانون بالتصرف فيها، سواء في استمرار الحفظ بقصد عرضها على الجهات القضائية المختصة او مصادرتها (بحكم قضائي عادة) او – كذلك – قد ينتهي بها الحال الى الإفراج عنها وأعادتها الى أصـــحابها إذا لم تكن ذات شـــأن في الجريمة المرتكبة.

---

[57] **Patrick S. Chen - An Automaic System for Collecting Crime Information on the the Internet - 31 October 2000 - Journal of information law and Technonlogy - available online in jan 2001 at: http://elj.warwick.ac.uk/jilt/00-3/chen.html**

[58] **US v. Gregory James Grant , No. 99 – 2332 , July 17 , 2000 . op cit**

وفي إطار جرائم الانترنت فإنه يميز بين الأدلة التي يلزم التحفظ عليها داخل الحاسوب، وبين تلك التي يلزم بقاؤها في العالم الافتراضي، وبين – أيضا – تلك النوعية من الأدلة التي تنتمي الى العالم الرقمي ومع ذلك يمكن اللجوء الى إخراجها من إطار الحاسوب والعالم الرقمي الى العالم المادي بحيث يتم التعامل معها كمخرجات يقبلها القضاء كأدلة كاملة في الجريمة تساعد في الإدانة وكذلك في البراءة.

إن التحفظ على الأدلة داخل الحاسوب Locating computer evidence من العمليات المعقدة التي تحتاج بداية الى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الحاسوب، وهذا الأمر يستلزم بالضرورة قيام الخبير التقني بالكشف بداية على المدى الذي عليه صحة حركة الحاسوب سيما من حيث الخلل والعطب. ويعطي العدوان الفيروسي مثالا حيويا هنا، إذ يكفي ان يكون هناك فيروس في الجهاز لكي يتم التشكيك في صحة الأدلة المستقاة من هذا الحاسوب، ومثل هذا الاتجاه نجده في التشريع الإنجليزي.

وتتم عملية حفظ الأدلة داخل الحاسوب بأساليب متعددة تتشكل في أبسط مظاهرها باستخدام أسلوب الحفظ العادي وأقوى مظاهرها في عمليات حجز الحاسوب على الدليل الموضوع فيه. ذلك إن الدليل الرقمي هو في العادة ملف يحتوي على بيانات رقمية تعطي مظهرا معلوماتيا محددا غير قابل للتحويل الى مظهر أخر، سوى حين القيام بإجراء تعديلات رقمية في البيانات المذكورة.

وإذا تأملنا عملية حفظ الأدلة في العالم الرقمي فإنه يتطلب من الخبير التقني القيام برصد موقع الانترنت او المعلومات التي تشير الى الجريمة، والتي تكون في مظاهر مختلفة الأشكال، كما لو كانت الجريمة من جرائم القذف والسب في غرف المناقشة، ففي مثل هذه الحالة الأخيرة يتم اللجوء الى ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي لكي يمكن التوصل الى تحديد موضوع السب والقذف وتاريخه. وإذا كانت الجريمة من جرائم النشر عبر الانترنت فقد يُكتفى بمجرد اللجوء الى ذاكرة الحاسوب المستخدم هنا دون حاجة الى تحديد الخادم.. الخ. ففي مثل هذه الحالات يقوم الخبير باستخدام برمجيات مساعده للتوصل الى القيام بالحفظ في العالم الرقمي، كما هو الشأن في حجز وتشفير مثل هذه المواقع بعد تحديد جدليتها ودقتها ومسارها، وهذا أمر يترتب عليه عدم إمكانية حذفها في العالم الرقمي، وإذا قام أحدهم بذلك فإنه يكون قد ارتكب جريمة.

وتستدعي عملية حفظ الأدلة في العالم الرقمي لزوم قيام الخبير بعرض الأدلة في المحكمة او على جهات التحقيق، ومثل هذا الأمر يجعل عمل الخبير يستمر لمرحلة المحاكمة وأحيانا يتطلب منه ذلك القيام بعمله لمرحلة ما بعد المحاكمة كما هو الشأن حال عرض الدليل المقدم الى محكمة الموضوع امام جهة قضائية أعلى كالاستئناف او النقض (في حالة اختصاصها بالموضوع – الطعن مرتين). ودرءا للمشكلات التي يمكن أن تنجم عن حفظ الأدلة في العالم الرقمي فإن العديد من المحاكم لجأت الى ميكنة إداراتها رقميا، بحيث يتم تسليم الأدلة الى إدارة متخصصة تتولى بدورها حفظ الأدلة في العالم الرقمي لعرضها على القضاء كلما تطلب الأمر ذلك.

وعملية الحصول على مخرجات الحاسوب والانترنت بقصد تقديمها كدليل في المحكمة تعد من أولى الموضوعات التي تعرض لها الفكر القانوني سواء من حيث قابليتها القانونية او من حيث منهجية الدليل الذي تم تخريجه، حتى ان هذه الطريقة تعد في المرحلة المعاصرة من الأساليب التقليدية في مجال الحصول على الدليل الرقمي. إذ يصح في القانون أن يكون هناك من الأدلة ما هو مخرج من مخرجات الحاسوب والانترنت، بحيث تعد هذه المخرجات أدلة أصلية على الرغم من كونها نسخ من دليل أصله موجود في العالم الافتراضي او في الحاسوب، فتعامل هذه المخرجات على هذا النحو. والأمثلة الدارجة في هذا الإطار ممثلة في الأدلة الناجمة عن العدوان الإجرامي على حقوق الملكية الأدبية والفكرية. حيث تعد النسخ التي

يتم تخريجها من المصنفات وطرحها في شكل ورقي او تسجيلات أدلة أصلية هنا، إذ يمكن مثلا طباعة نسخة من مصنف او عنوان مصنف او علامة تجارية او براءة اختراع او غير ذلك تم العدوان عليه إجراميا وانتزاع حق المؤلف عنه وبالتالي عرضه كدليل على القضاء دون حاجة للتدقيق في مدى أصالتها ما دامت قد تم تخريجها من حاسوب غير معطوب او مصاب بخلل برمجي.

ويقوم الخبير بتخريج هذه المخرجات الى العالم المادي بطرق مختلفة أبرزها في العمل هي الطباعة على الطابعة Print Out، وذلك بتحويلها الى نسخ ورقية عوضا عن كونها رقمية او نبضية. والخبير في ذلك لا يكتفي بمجرد نسخ البعض المعلوماتي وانما يحتاج أيضا الى تخريج النبض البياناتي بحيث يقوم بتخريج كافة البيانات الرقمية حين طباعة هذا الدليل.

ومخرجات البيانات هي الأصل الرقمي للموضوع المعلوماتي دائما، بحيث لا يكون للمعلومة وجود ما لم يكن لها أصل رقمي يتم بمقتضاه هيكلة المعلومة. ومن أمثلتها ذات الحيوية الفائقة قواعد البيانات Data Base حيث يكون لها دور كبير في رصد المعلومات المراد عرضها عبر الانترنت. ومن التطبيقات الدارجة في هذا الإطار سجل الزيارات Gust Book الذي يتم رصده في أغلب المواقع والصفحات عبر الانترنت، حيث يكون هذا السجل معدا بطريق قاعدة البيانات فيعطي الفرصة الكاملة لصاحب الموقع في اختيار الكلمات المعدة للنشر وحذف ما عدا ذلك سيما تلك غير اللائقة. وفي هذه الحالة يقوم الخبير برصد قاعدة البيانات باستخدام الشفرة الملائمة وإنزال Download وطباعة قاعدة البيانات كمخرجات بقصد تقديمها الى المحكمة.

الرابع - القيود التي ترد على عمل الخبير التقني: - من الأهمية بمكان التقرير بأن عمل الخبير التقني من أعمال الخبرة غير المطلقة في طبيعتها، وبالتالي يلتزم الخبير التقني بما هو مقرر في مفاهيم المشروعية التي يعترف بها القانون كحقوق للإنسان ويقرها القضاء كمنهج عمل يدافع به عن الانسان في كل مكان. ويظل الأمر هنا مرتبطا بالمشروعية في هذا المجال، إذ ليس للخبير أن يلجأ الى أساليب غير مشروعة من أجل القيام بعمله.

ولعل من الأساليب ذات الخطورة الخاصة في عمل الخبير التقني هي الدراسات التاريخية التي يقوم بها الخبير، قصد تحديد أسلوب مرتكب الجريمة، وهي دراسات محاطة بالسرية المطلقة في هذا المجال لكونها تؤدي الى فتح سجلات وملفات انتهى موضوعها، او إنها تجعل الخبير يطلع على محاضر تحقيقات قد ينص في التشريعات على حظر اطلاع غير سلطات التحقيق عليها، سيما في الحالات التي يكون فيها الخبير خبيرا في قضية أخرى ليست ذات علاقة بموضوع القضية التي يقوم بتحقيقها.

كذلك يكون للخبير أن يطلع على شهادات وأقوال الجناة في الصحف وأمام الجهات الرسمية والشعبية، إذ كثيرا ما يكون في مثل هذه الأقوال عوامل مساعدة لخبرته، فيمكن من خلالها التعرف على أسلوب عمل مرتكب الجريمة المعلوماتية والتعامل معه على أساس أقواله، ومعلوم إن الكونجرس الأمريكي قد استدعى أحد كبار هكرة العالم الافتراضي، بل وأخطرهم على الإطلاق، وهو كيفين ميتنيك، لكي يدلي بشهادته كـ.. هاكر عن كيفية ارتكابه للاختراق ورأيه في اعداد تشريع يحظر الاختراق. ولقد تضمنت شهادته العديد من الامور التي كانت خافية على رجال التشريع والقانون، بل وهي كشهادة من مجرم عدت سابقة تشريعية في هذا المجال.

على أن من المشاكل التي يمكن ان تثار هنا تتعلق بمدى إمكانية قيام الخبير التقني بالاستعانة بهكرة ومرتكبي جرائم رقمية او معلوماتية وإن كان ذلك يتم في الغالب بشكل سري؟

ومثل هذه المسألة سوف تطفو على سطح الأحداث، فالكونجرس لم يأت بهذه الفكرة من فراغ، حيث كونه يمثل الشعب الامريكي، ومن ثم فإن هذه الخطوة لن تحسب على الكونجرس الامريكي ذاته بقدر ما تعبر عن اتجاهات الرأي العام في هذا الشأن. سيما ازاء وجود ظاهرة تعاقد القطاع الخاص مع الهكرة وهي دعوة كانت قد قامت في منتصف 1999 من قبل كبار الشركات تجنبا لاختراقاتهم، وبحيث تعد تدبيرا وقائيا نوعيا جديدا يمكن أن يحقق – كمسعى في ذلك الوقت – تناقصا في جرائم الاختراق. لذلك فإن عمل الخبير القضائي يمكن أن يحقق نوعا ما نتيجة هامة في تفعيل دور الدراسات التاريخية للهكرة وجرائمهم وهذا يعني لزوم تفاعل علم الأجرام مع عمل الخبير التقني، فيتولى القيام برصد تاريخي لحركة هذا او ذاك الهاكر ومحاولة التعرف على أسلوبه لكي يمكن معرفة وتتبع الخطوات التقنية التي يقوم بها والتي قد يقوم الغير بسلوكها. ويظل الفيصل في هذه المسألة في مدى تقبل القضاء لدليل مستمد من استعانة الخبير بهكرة؟

إن استعانة خبير قضائي بمجرم معلوماتي للتعرف على أسلوب ارتكاب جريمة معلوماتية لا يجعل من الهاكر خبيرا في الدعوى، إذ إن التقييم المعلوماتي يظل هنا للخبير القضائي ثم لقاضي الموضوع في نهاية المطاف. وما دور الهاكر الا دور مساعد للخبير، وللخبير أن يطلب مساعدة من يشاء في هذا الإطار، على إن المساعدة المطلوبة في هذه الحالة تكون من مجرم سيما إذا كان مطلوبا للعدالة في جريمة أخرى مرتكبة؟

إن ما قام به الكونجرس الامريكي من استدعاء لاحد كبار الهكرة للإدلاء بشهادته أمامه تعد سابقة على درجة كبيرة من الخطورة امام الجهة التشريعية التي تعد ممثلا للشعب هنا. وهذه السابقة في القانون المقارن سوف تقود الى تظاهرة قانونية تبدأ من مدى دستورية استدعاء مؤتمر الشعب العام الامريكي لمجرم للإدلاء بشهادته أمامه؟ فهل يملك الشعب استدعاء مجرم - حتى وان كان قد أنهى عقوبته - للإدلاء بشهادته أمامه.

الدليل الرقمي

في قانون الاجراءات الجنائية الجديد

DIGITAL EVIDENCE
& THE NEW CRIMINAL PROCEDURE

البروفيسور اورين كير

Prof. Orin S. Kerr[1]*

[1] Associate Professor, George Washington University Law School. Thanks to John Duffy, Laura Heymann, Mark Lemley, Cynthia Lee, Chip Lupu, Dan Markel, Tom Morgan, Julian Mortenson, Spencer Overton, Steve Schooner, David Sklansky, Daniel Solove, Peter Swire, and Bob Tuttle for their helpful comments on a prior draft.

الدليل الرقمي في قانون الاجراءات الجنائية الجديد

DIGITAL EVIDENCE AND THE NEW CRIMINAL PROCEDURE

البروفيسور اورين كير

Orin S. Kerr[2]*

أدى الاستخدام الواسع النطاق widespread use لأجهزة الحاسوب في السنوات الأخيرة إلى نوع جديد من الأدلة في القضايا الجنائية: الأدلة الرقمية digital evidence، وتتكون من الأصفار والاحاد بالنبض الكهربائي consisting of zeros and ones of electricity. وفي هذا المقال، ينظر البروفيسور "كير" فيما إذا كانت القواعد التقليدية للإجراءات الجنائية أن تنظم بشكل فعال التحقيقات التي تنطوي على أدلة رقمية. ويخلص "كير" إلى أن الأساليب الجديدة لجمع الأدلة الرقمية تثير الحاجة إلى معايير قانونية جديدة. والقانون الحالي مصمم خصيصا لجمع الأدلة المادية وشهادات شهود العيان؛ ويؤدي تطبيق هذا القانون على جمع الأدلة إلى عدد من النتائج المدهشة. يؤكد البروفيسور "كير" أن هناك حاجة إلى قواعد جديدة، ويقدم أفكارا أولية حول كيف يجب أن تبدو هذه القواعد وما هي المؤسسات التي يجب أن تولدها.

[2] Associate Professor, George Washington University Law School. Thanks to John Duffy, Laura Heymann, Mark Lemley, Cynthia Lee, Chip Lupu, Dan Markel, Tom Morgan, Julian Mortenson, Spencer Overton, Steve Schooner, David Sklansky, Daniel Solove, Peter Swire, and Bob Tuttle for their helpful comments on a prior draft.

مدخل

I. دليل مادي ضد دليل رقمي:
   a. جرائم مادية والتحقيق في الجرائم المادية.
   b. جرائم حاسوب وجريمة حاسوب.
II. ادلة رقمية وفشل القواعد النافذة:
   a. جرائم مادية/ تقليدية وقواعد الاجراءات الجنائية.
   b. دليل رقمي وقواعد العالم المادي.
   c. دليل من أطراف ثالثة واجراء اذن التفتيش.
   d. المراقبة المستقبلية ومشكلة التصنت السلكي/ الهاتفي.
   e. تفتيش الحاسوب المستهدف وقواعد اذن التفتيش.
III. باتجاه قواعد جديدة للإجراءات الجنائية:
   a. تجميع الدليل المخزن لدى أطراف ثالثة.
   b. المراقبة المستقبلية.
   c. اجراء المعمل الشرعي الحاسوبي.
   d. خلاصة.

مقدمة

INTRODUCTION

تتناول هذه الدراسة كيف يجب أن يتغير قانون الإجراءات الجنائية استجابة للعدد المتزايد من القضايا الجنائية التي تستند بشكل كبير إلى الأدلة الرقمية[3]. وتجادل بأن استخدام أجهزة الحاسوب في النشاط الإجرامي قد أشاع شكلا جديدا من الأدلة، الأدلة الرقمية، وتشرح كيف يختلف جمع الأدلة الرقمية عن تقنيات التحقيق التقليدية. وتدعي أن الأساليب الجديدة لجمع الأدلة الرقمية ينبغي ويجب أن تؤدي إلى إصلاحات في قانون الإجراءات الجنائية لتنظيم جمع الأدلة الرقمية.

يجب أن تؤدي الأدلة الرقمية إلى قواعد جديدة للإجراءات الجنائية لأن الجرائم المتعلقة بالحاسوب تتميز بحقائق جديدة تتطلب قانونا جديدا. وقد تطور قانون الإجراءات الجنائية لتنظيم الآليات المشتركة للتحقيق في الجرائم المادية، وهي جمع الأدلة المادية وشهادات شهود العيان. تم تصميم القانون الحالي بشكل طبيعي لتلبية احتياجات السلطات وتهديدات الخصوصية التي تثيرها. حيث يتم جمع الأدلة الرقمية بطرق مختلفة عن شهادة شهود العيان أو الأدلة المادية. تختلف الطرق الجديدة لجمع الأدلة اختلافا كبيرا لدرجة أن القواعد التي تم تطويرها للتحقيقات القديمة لم تعد منطقية في كثير من الأحيان بالنسبة للتحقيقات الجديدة. اذ انها غالبا ما تؤدي تلك القواعد التي توازن بين الخصوصية والسلامة العامة عند تطبيقها على وقائع التحقيقات في الجرائم المادية إلى نتائج مذهلة عند تطبيقها على الأساليب الشائعة في تحقيقات الأدلة الرقمية. فهي تسمح للسلطات الحكومية الغازية invasive government powers بشكل غير عادي بأن تصبح غير منظمة في بعض السياقات، ومع ذلك تسمح لتهديدات الخصوصية الوهمية بإغلاق التحقيقات المشروعة في سياقات أخرى.

تؤكد هذه الدراسة أن الديناميات الجديدة new dynamics تظهر الحاجة إلى مذاهب إجرائية مصممة خصيصا لتنظيم جمع الأدلة الرقمية. حيث انها يجب أن تفرض القواعد بعض القيود الجديدة على سلوك الشرطة/ مأمور الضبط القضائي وإلغاء القيود الأخرى مع مراعاة الحقائق الجديدة والممارسات الاجتماعية الجديدة الشائعة في كيفية استخدامنا لأجهزة الحاسوب وإساءة استخدامها misuse computers. علاوة على ذلك، يجب أن ننظر إلى ما وراء القضاء والتعديل الرابع للعديد من هذه القواعد الجديدة. في حين أن بعض التغييرات يمكن أن تأتي من المحاكم، ومن المحتمل أن تأتي، ويمكن أن يأتي المزيد من الهيئات التشريعية والوكالات التنفيذية القادرة على تقديم نهج جديدة ومبتكرة لا ترتبط مباشرة بتقاليدنا الدستورية constitutional traditions.

وقد بدأت بالفعل بعض التغييرات. بدأ عدد من القواعد الجديدة في الظهور من الكونغرس والمحاكم. في السنوات الخمس الماضية، بدأت بعض المحاكم في تفسير التعديل الرابع بشكل مختلف في قضايا جرائم الحاسوب. ولقد تم رفض القواعد التقليدية بهدوء وتم استبدالها بالقواعد الجديدة. وعلى المستوى التشريعي، سن الكونجرس قوانين خاصة بالحاسوب لمعالجة التهديدات الجديدة الأخرى للخصوصية. التغييرات

[3] Criminal procedure is generally defined as the rules and procedures that the police and prosecutors must follow as they investigate and prosecute criminal activity. See, e.g., Russell Weaver et al., Criminal Procedure: Cases and Materials 2 (2001)

متواضعة حتى الآن. ومع ذلك، يمكن النظر إلى القواعد الدستورية والقانونية الجديدة مجتمعة على أنها بداية لحقل فرعي جديد من الإجراءات الجنائية ينظم جمع الأدلة الرقمية.

وتستمر هذه الدراسة في ثلاثة أجزاء. ويقارن الجزء الأول الآليات الأساسية للجرائم التقليدية والجرائم ذات الصلة بالحواسيب. ويشرح كيف أن التحول من الجرائم المادية physical crimes إلى الجرائم الإلكترونية electronic crimes يؤدي إلى التحول من الأدلة المادية physical evidence وشهادة شهود العيان eyewitness testimony إلى الأدلة الرقمية digital evidence، وكيف يميل المحققون إلى استخدام طرق جمع مختلفة جدا لهذين النوعين من الأدلة. يتحول الجزء الثاني من الحقائق facts إلى القانون الحاكم governing law، مع التركيز على حظر التعديل الرابع لعمليات التفتيش والضبط غير المعقولة unreasonable searches and seizures. ويبين أن مبدأ التعديل الرابع الحالي مصمم بشكل طبيعي لوقائع الجرائم المادية، ولكن هناك عددا من الصعوبات التي تنشأ عندما يتم تطبيق هذا المبدأ على وقائع التحقيقات في جرائم الحاسوب. يجادل الجزء الثالث بأن هناك حاجة إلى قواعد جديدة لتنظيم جمع الأدلة الرقمية، ويقدم أفكارا أولية حول الشكل الذي قد تبدو عليه هذه القواعد والمؤسسات التي يجب أن تنشئها. كما يظهر أن المحاكم والكونغرس قد بدأوا بالفعل في الاستجابة لمشكلة الأدلة الرقمية بعدد من القواعد الخاصة بالحاسوب.

I. الدليل المادي في مواجهة الدليل الرقمي

I. PHYSICAL EVIDENCE VERSUs DIGITAL EVIDENCE

ان قواعد الإجراءات الجنائية Rules of criminal procedure هي قواعد أساسية organic rules، تتوقف على وقائع التحقيقات التي تنظمها. وتمارس وضعية تغيير الحقائق ضغوطا لتغيير العقيدة القانونية القائمة existing legal doctrine. ولمعرفة السبب في أن الأدلة الرقمية تخلق ضغطا من أجل قواعد جديدة للإجراءات الجنائية، نحتاج إلى البدء بمقارنة حقائق التحقيق في الجرائم التقليدية بوقائع التحقيق في الجرائم التي تنطوي على أدلة رقمية. سوف يستكشف هذا الجزء الاختلافات من خلال مقارنة مثالين. المثال الأول هو سرقة بنك تقليدية. والمثال الثاني هو جريمة حاسوب مماثلة تقريبا حيث يسرق المشتبه به الأموال عن طريق اختراق hacking جهاز حاسوب مصرفي. ومن خلال مقارنة هاتين الجريمتين، يمكننا أن نرى كيف أن آليات mechanisms الجرائم الإفتراضية Cybercrime والجرائم المادية غالبا ما تكون متميزة. تؤدي هذه الآليات المختلفة إلى أدلة مختلفة، وخطوات تحقيق مختلفة، وفي نهاية المطاف، الحاجة إلى قواعد قانونية مختلفة.

A. جرائم العالم المادي والتحقيقات في جرائم العالم المادي

A. Physical Crimes and Physical Crime Investigations

تخيل أن فريد فيلوني Fred Felony قرر سرقة أحد البنوك. يقود فريد سيارته إلى مكتب فرعي محلي، ويوقف سيارته في الخارج، ويدخل. عندما يحين دوره امام الصراف teller، ينزلق فريد فوق ملاحظة تقول، "هذه معضلة stick up. أعطني كل الأموال ولن يصاب أحد بأذى". يرى الصراف الملاحظة ويلاحظ قبضة مسدس بارز من سترة فريد. يسلم الصراف بعصبية فريد حقيبة من المال. يمسك فريد بالحقيبة وينفد من البنك. بمجرد خروجه، يقفز إلى سيارته حيث يهرب ويبتعد بسرعة.

تخيل الآن أن يتم استدعاء محقق شرطة police detective للتحقيق investigate في سرقة البنك. وهدف المحقق هو جمع الأدلة على الجريمة حتى يتمكن من التعرف على السارق ثم المساعدة في إثبات القضية في المحكمة بما لا يدع مجالا للشك[4]. ولكن كيف ستكون الاستراتيجية الأولى للمحقق وهي جمع شهادات شهود العيان؟ سيطلب المحقق من الصراف والأشخاص الآخرين في البنك وصف ما لاحظوه. كيف بدا السارق؟ كم كان طوله؟ هل كان صوته غير عادي؟ هل رأى أحد سيارة الهروب؟ ستتألف شهادة شهود العيان من تقارير من أشخاص حول ما لاحظوه بأعينهم وسمعوه بآذانهم. من خلال زيارة البنك وطرح الأسئلة، سيصبح المحقق شاهد عيان من نوع ما: سيكون قادرا على الإدلاء بشهادته حول ما رآه وسمعه عندما وصل إلى البنك وحقق في الجريمة.

ستكون الاستراتيجية الثانية للمحقق هي جمع الأدلة المادية. سوف تساعد الأدلة المادية في ربط الجريمة بالمشتبه به بما لا يدع مجالا للشك. وعلى سبيل المثال، سيستعيد المحقق الملاحظة التي تركها فريد فيلوني مع الصراف ويحللها بحثا عن بصمات الأصابع أو خط اليد المميز. ربما ترك فريد وراءه أدلة جسدية أخرى أيضا. ربما أسقط البندقية عندما هرع خارج البنك. ربما فقد زرا، أو أسقط إيصالا كان يحمله في جيبه. يمكن تقديم هذه الأدلة المادية وشرحها إلى هيئة المحلفين لإنشاء صلة ملموسة قوية بين المتهم defendant والجريمة[5].

إذا لم تثبت شهادة شهود العيان eyewitness testimony والأدلة المادية physical evidence من البنك القضية ضد فريد، فقد تحتاج الشرطة إلى البحث عن أدلة إضافية في مكان آخر additional evidence elsewhere. قد تستجوب الشرطة مشتبها بهم آخرين لمعرفة ما إذا كانوا يعرفون من يقف وراء سرقة البنك. قد يبحثون في جميع أنحاء المدينة عن سيارات مطابقة لوصف سيارة الهروب. إذا كانت لدى الشرطة شكوك خاصة حول فريد، فيجوز لها تفتيش منزله بحثا عن أدلة مثل الأوراق النقدية المسروقة أو الملابس المطابقة لتلك التي يرتديها السارق. سيكون الهدف هو جمع شهادات شهود عيان إضافية وأدلة مادية يمكن أن تساعد في إثبات أن فريد سرق البنك. إذا أسفر أي من هذه التكتيكات عن أدلة إضافية، فستضيف الشرطة الأدلة الجديدة إلى الأدلة المادية وشهادات شهود العيان الموجودة في مسرح الجريمة crime scene.

لنفترض أن المحقق يجمع أدلة كافية لإثبات أن فريد ارتكب سرقة البنك. فريد متهم، والقضية تذهب إلى المحاكمة. وفي المحاكمة، يقوم المدعون العامون بتجميع شهادة شهود العيان والأدلة المادية لإثبات أن فريد ارتكب الجريمة. وسوف يشهد الصراف حول كيفية اقتراب فريد فيلوني منه وتسليمه المذكرة. وسيدلي شهود عيان eyewitnesses آخرون بشهاداتهم حول ما رأوه وسمعوه أثناء السرقة. سيساعد الشهود الذين هم على دراية شخصية بالأدلة المادية في رعايتها كدليل حتى تتمكن هيئة المحلفين jury من النظر فيها في غرفة هيئة المحلفين the jury room أثناء المداولات deliberations[6]. على سبيل المثال، إذا ألقى فريد مسدسه في طريقه للخروج من البنك ووجده المحقق، فسيأخذ المحقق الموقف ويشهد حول كيف وأين وجد المسدس. سيتم بعد ذلك قبول المسدس كدليل[7]. إذا نفذت الشرطة تفتيشا في منزل فريد فيلوني، فإن العميل الذي شارك

[4] See In re Winship, 397 U.S. 358, 363-64 (1970) (discussing the reasonable doubt standard).
[5] See, e.g., United States v. Patane, 124 S. Ct. 2620, 2631 (2004) (Kennedy, J., concurring) (noting "the important probative value of reliable physical evidence").
[6] Evidentiary rules such as Federal Rule of Evidence 901 guide the admission of evidence. Such rules normally require testimony "sufficient to support a finding that the matter in question is what its proponent claims," Fed. R. Evid. 901(a), such as by testimony from a witness with personal knowledge, id. 901(b)(1).
[7] See, e.g., United States v. Towns, 913 F.2d 434, 439 (7th Cir. 1990) (reviewing physical evidence admitted at trial following a bank robbery, including "a small blue vinyl bag similar to the one that [a] defendant

في التفتيش سيشهد حول ما وجده. سيؤدي تسلسل الشهود في المحاكمة إلى بناء القضية ضد فريد جناية ومحاولة إثبات ذنبه بما لا يدع مجالا للشك beyond a reasonable doubt.

B. جرائم الحاسوب والتحقيقات في جرائم الحاسوب

B. Computer Crimes and Computer Crime Investigations

الآن دعنا ننتقل إلى نسخة إلكترونية electronic version من هذه الجريمة. دعونا نستبدل الزيارة المادية للبنك واسترجاع النقود الورقية بـ.. "زيارة" افتراضية virtual visit للبنك وسرقة الأموال الرقمية من حاسوب البنك. الهدف من المقارنة ليس العثور على تناظرية دقيقة لسرقة البنك المادية. هناك اختلافات واضحة بين الاثنين[8]. وبدلا من ذلك، يكون الهدف هو التعرف على كيفية تغير الجريمة والأدلة عندما ننتقل من الجرائم المادية إلى الجرائم التي تنطوي على أدلة رقمية digital evidence.

هذه المرة، يقرر فريد فيلوني سرقة الأموال باستخدام جهاز حاسوب. بدلا من زيارة البنك شخصيا، يذهب عبر الإنترنت من منزله. يقوم فريد بتسجيل الدخول إلى الإنترنت من حساب يملكه مع مزود خدمة إنترنت محلي local internet service provider (ISP) على الرغم من أن هدفه النهائي هو اختراق أجهزة الحاسوب الخاصة بالبنك، إلا أن فريد يكرر هجومه أولا من خلال عدد قليل من أجهزة الحاسوب الوسيطة لإخفاء مساراته. يختار أجهزة الحاسوب ذات الأمان الضعيف والحاجة القليلة للاحتفاظ بسجلات مفصلة لمن استخدم خوادمهم. إذا حاول أي شخص تتبع سوء سلوك فريد إليه، فسيتعين عليه المرور عبر الوسطاء أولا. لنفترض أن فريد اختار خادما تديره جامعة خاصة في كاليفورنيا كوسيط أول له، وخادم تديره مكتبة عامة في كانساس كوسيط ثان له. من مزود خدمة الإنترنت ISP الخاص به، اخترق hack أولا حاسوب الجامعة. مع إنشاء وصول إلى حاسوب الجامعة، قام بعد ذلك باختراق حاسوب المكتبة. مع إنشاء وصول إلى حاسوب المكتبة، يستهدف فريد الخادم الرئيسي للبنك bank's main server. وبعد عدة محاولات، يخمن فريد في النهاية كلمة المرور الرئيسية بشكل صحيح ويسجل الدخول إلى خادم البنك. قد يبدو الرسم التخطيطي للهجوم كما يلي:

[was carrying during the bank robbery,] an empty ammunition clip that would fit only a .44 caliber magnum semi-automatic pistol" that was recovered from hotel room where defendant stayed on the night of the robbery, as well as "a pair of sunglasses similar to those that defendant Towns allegedly wore during the bank robbery; and . . . several money wrappers that were identical to those that had bound the money that the robbers had taken from the bank").

[8] The most obvious difference is that the physical crime involves a threat of physical harm to persons. In the language of criminal law, the physical crime is a robbery; the virtual crime is a form of bank theft. See generally Wayne R. LaFave, Criminal Law 996 (4th ed. 2003) (noting that the crime of robbery "may be thought of as aggravated larceny-misappropriation of property under circumstances involving a danger to the person as well as a danger to property-and thus deserving of a greater punishment than that provided for larceny" (citations omitted)).

فريد- مزود الخدمة- الجامعة- المكتبة- البنك

Fred - ISP - University -- Library – Bank

ومع امتيازات النظام الكاملة على حاسوب البنك، يقوم فريد بإعداد حساب مصرفي جديد ويوجه instructs الحاسوب إلى أن الحساب يحتوي على 500000 دولار. ثم يقوم بتحويل الأموال من الحساب الجديد إلى حساب خارجي لا يمكن تعقبه. وفي اليوم التالي، لاحظ موظف البنك bank employee أنه تم إنشاء حساب غير مصرح به unauthorized account وأن الأموال مفقودة. يتصل موظف البنك بالشرطة[9].

تخيل أن القضية قد تم تعيينها لنفس المحقق detective الذي حقق في سرقة البنك المادية physical bank robbery. مرة أخرى، وهدفه هو جمع أدلة كافية لتحديد الجاني wrongdoer وإقامة قضية امام المحكمة. لكن كيف؟ سيلاحظ المحقق على الفور أن مسرح الجريمة crime scene يبدو مختلفا تماما. لا يوجد شهود عيان في البنك، ولا يوجد دليل مادي. لم ير أحد حدوث الاقتحام، ولا يوجد دليل ملموس للتلاعب. من وجهة نظر الحواس البشرية، وقعت الجريمة داخل أسلاك وصناديق مغلقة عن طريق التحول السريع للنبضات الكهربائية غير المرئية والصامتة. ويمكن لفنيي الحاسوب ومسؤولي النظام البحث في ملفات الحاسوب ومحاولة إعادة بناء ما حدث. حيث يمكنهم مراقبة ما تظهره لهم شاشات الحاسوب الخاصة بهم. لكن الدليل الأساسي لم يعد شهادة شهود عيان أو أدلة مادية. إنه دليل رقمي digital evidence: أصفار واحاد من طبيعة كهربائية.It is digital evidence: zeros and ones of electricity .

كيف تبدأ التحقيق؟ ستكون الخطوة الأولى للمحقق هي مطالبة مسؤول النظام المسؤول عن حاسوب البنك بجمع جميع المعلومات المتعلقة بالسرقة التي قد يتم تخزينها على الحاسوب. وفي جميع الاحتمالات، ستخبره هذه المعلومات بالقليل جدا. ومع الجريمة المادية، فقد كانت هناك فرص جيدة في أن يسفر مسرح الجريمة crime scene عن خيوط كبيرة substantial leads. حتى لو لم يتمكن أحد من التعرف على فريد في تشكيلة عرض المشتبه بهم number of suspects، فإن وجوده المادي في مسرح الجريمة ضيق إلى حد كبير عدد المشتبه بهم. ويبدو مسرح الجريمة الافتراضية مختلفا تماما. ففي معظم الحالات، ستخبر الأدلة التي تم جمعها في موقع الضحية المحقق فقط أن شخصا ما، يتواجد في مكان ما في العالم، قام باختراق البنك hacked into the bank.

في معظم القضايا، يأتي أكبر دليل تحقيق investigative lead في شكل عنوان بروتوكول إنترنت Internet Protocol (IP) مسجل بواسطة خوادم البنك. عنوان بروتوكول الانترنت IP هو ما يعادل رقم الهاتف على الانترنت[10]؛ ومن المحتمل أن يكون خادم البنك قد احتفظ بسجل لاتصال فريد بجهاز الحاسوب الخاص بالبنك وسجل عنوان بروتوكول الانترنت IP الأصلي الخاص به كجزء من هذا السجل. وللعثور على Fred Felony، يجب أن يبدأ المحقق بعنوان IP ويحاول تتبع أثر فتات الخبز الإلكتروني من البنك

[9] This hypothetical is loosely based on a case from 1995. A computer hacker named Vladimir Levin, located in St. Petersburg, Russia, hacked into Citibank computers, set up various accounts, filled them with money, and then had coconspirators withdraw the money. See, e.g., William M. Carley & Timothy L. O'Brien, How Citicorp System Was Raided and Funds Moved Around World, Wall St. J., Sept. 12, 1995, at Al.

[10] See generally Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 407 n.4 (2d Cir. 2004) (posthumously published draft opinion of Parker, C.J.) (defining an Internet Protocol address as "[t]he unique identification of the location of an end-user's computer [which] serves as a routing address for email and other data sent to that computer over the Internet from other end-users").

electronic bread crumbs إلى حاسوب فريد المنزلي[11]. ويجب عليه العثور على أجزاء وبايتات وبيتات bits من الأدلة الرقمية المخزنة في جميع أنحاء البلاد (إن لم يكن في جميع أنحاء العالم) وجمعها بطريقة تحدد فريد وتثبت ذنبه بما لا يدع مجالا للشك.

وتنقسم عملية جمع الأدلة الإلكترونية electronic evidence في قضايا هكترة الحاسوب عموما إلى ثلاث خطوات. يبدأ بجمع الأدلة المخزنة من خوادم الطرف الثالث، ويتحول إلى جانب المراقبة المحتملة prospective surveillance، وينتهي بالتحقيق الجنائي لجهاز الحاسوب الخاص بالمشتبه به. تشمل هذه الخطوات الثلاث الآليات الأساسية لجمع الأدلة الرقمية: جمع الأدلة الرقمية أثناء النقل، وجمع الأدلة الرقمية المخزنة لدى أطراف ثالثة صديقة، وجمع الأدلة الرقمية المخزنة مع أطراف معادية مثل الهدف. تقدم كل آلية حقائق فريدة وتتطلب اعتبارات خاصة.

تتمثل خطوة التحقيق الأولى والأساسية most basic investigative step في الحصول على السجلات المخزنة stored records من مسؤولي النظام لمختلف خوادم الحاسوب المستخدمة في الهجوم. قام فريد بالاتصال بأربعة أجهزة حاسوب لارتكاب جريمته: خوادم يديرها مزود خدمة الإنترنت ISP servers والجامعة والمكتبة والبنك. من الممكن (وإن لم يكن مؤكدا although not certain) أن يحتفظ كل من هذه الخوادم بسجلات اتصال فريد. سيحاول المحقق تجميع هذه السجلات لتتبع الهجوم من خادم البنك عبر أجهزة الحاسوب الوسيطة إلى مزود خدمة الإنترنت بطريقة خطوة بخطوة.

هذا الإجراء المرهق cumbersome procedure ضروري لأن الحزم packets التي تحمل اتصالات الإنترنت تسرد فقط نقاط المنشأ والوجهة المباشرة[12]. فإذا شن فريد هجوما من مزود خدمة الإنترنت الخاص به عبر خوادم الجامعة والمكتبة ثم إلى بنك الضحية، فإن الاتصالات المستلمة على حاسوب البنك ستحمل عنوان بروتوكول الانترنت IP الأصلي لخادم المكتبة، ليس مزود خدمة الإنترنت ISP الخاص بفريد.

يجب على المحقق الاتصال بمسؤول النظام في المكتبة لتحديد ما إذا كان لديهم أي سجلات للاتصال بالبنك في الوقت المحدد الذي وقع فيه الهجوم. وفي حالة وجود سجلات records شاملة في المكتبة، يجب أن تشير هذه السجلات إلى أن الهجوم على البنك نشأ في الجامعة. سيقوم المحقق بعد ذلك بتكرار العملية عن طريق الاتصال بمسؤول النظام في الجامعة. وفي حالة وجود سجلات شاملة في الجامعة، ستشير هذه السجلات إلى أن الهجوم لم ينشأ في الجامعة، ولكن في مزود خدمة الإنترنت الخاص بفريد. سيقوم المحقق بعد ذلك بالاتصال بمزود خدمة الإنترنت الخاص بفريد. إذا كانت هناك سجلات شاملة في مزود خدمة الإنترنت، فيجب أن تشير هذه السجلات إلى أن حساب فريد كان يستخدم للوصول إلى الإنترنت وقت الهجوم. اذ يجب

[11] Cf. Michael L. Rustad, Private Enforcement of Cybercrime on the Electronic Frontier, 11 S. Cal. Interdisc. L.J. 63, 98 (2001) (noting that for investigators of internet crimes there are no geographical borders and thus there is no "traditional crime scene").

[12] Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 663 (2003) [hereinafter Kerr, Internet Surveillance]. This is true because the internet is a packet-switched network, and a communication intentionally sent from A to B to C is normally routed via two different stages of packets: First, a packet is made to send the information from A to B, then at B a new packet is created to send the communication from B to C. As a consequence of this architecture, the packet only indicates the source of the most recent packetizing. See id. at 663 n.284.

أن يكون لدى مزود خدمة الإنترنت أيضا بطاقة ائتمان أو عنوان إرسال فواتير لفريد في سجلاته، مما يسمح للمحقق بتركيز التحقيق على فريد"[13].

ومع ذلك، فانه نادر ما تكون التحقيقات بهذه البساطة. عادة ما يتم قطع مسار الأدلة في مكان ما على طول الطريق. اذ يحتفظ عدد قليل من مسؤولي النظام بسجلات شاملة، وغالبا ما يتم حذف تلك السجلات التي يتم الاحتفاظ بها بعد فترة زمنية وجيزة[14]. ويستهدف المتسللون بشكل روتيني أجهزة الحاسوب الوسيطة المعروفة باحتفاظها بسجلات قليلة أو معدومة لإحباط المحققين. عندما تحتوي سلسلة السجلات المخزنة على رابط مكسور، يجب على المحقق أن يحول التروس إلى طريقة ثانية لجمع الأدلة في مكان آخر تسمى المراقبة المستقبلية[15]. وتشير المراقبة المستقبلية إلى استخدام برامج أو أجهزة تسجيل لمراقبة حركة المرور على الإنترنت في المستقبل وإنشاء سجل لحركة المرور هذه. ويعتمد نطاق المراقبة المستقبلية على مكان تركيب جهاز المراقبة وكيفية تكوينه. قد يشمل التنصت على المكالمات الهاتفية الغازية التي تعترض رسائل البريد الإلكتروني الخاصة، أو قد تشير فقط إلى عنوان المصدر الأكثر إلحاحا للهجوم.

والفكرة الأساسية وراء المراقبة المستقبلية هي أن النشاط الإجرامي قد يتكرر reoccur أو يكون مستمرا ongoing، ويمكن للمحققين ومسؤولي نظام الضحايا إكمال الحلقات المفقودة في سلسلة الأدلة من خلال مراقبة النشاط المستقبلي. قد يعود فريد لمحاولة إنشاء حساب آخر وسحب المزيد من الأموال. إذا أصبح مسار الأدلة باردا في خادم البنك نفسه، فيمكن للبنك مراقبة خادمه بحثا عن الجهود غير المصرح بها لإنشاء حساب. إذا أصبح المسار باردا في الجامعة، يجوز للشرطة تركيب جهاز مراقبة في خادم الجامعة لمراقبة أي اتصالات موجهة من الخادم إلى البنك. إذا ارتكب فريد جناية مرة أخرى، يمكن للمراقبة المحتملة أن تخلق مسارا جديدا من الأدلة إلى مزود خدمة الإنترنت ISP الخاص بفريد[16].

وهذا يقودنا إلى المرحلة الثالثة والأخيرة من جمع الأدلة الإلكترونية electronic evidence. تذكر أنه في حالة جريمة فريد المادية، كان من الممكن أن تحتاج الشرطة إلى تنفيذ أمر تفتيش في منزله لجمع أدلة كافية

---

[13] For example, in United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000), FBI investigators determined that a computer assigned the IP address 24.94.200.54 contained illegal images of child pornography. Investigators contacted Road Runner, the ISP that controlled this IP address, and obtained the following information: The subscriber whose computer used I.P. address 24.94.200.54 on July 2, 1999, at 11:49 p.m. was Rosemay (sic) D. Kennedy of 9120 Harvest Court, Wichita, Kansas, telephone 316-722-6593. Two users were listed for that account: RKENNEDY@KSCable.COM and KENNEDYM@KSCable.Com. The account had been active since June 7, 1999.
Id. at 1107.

[14] See Computer Crime and Intellectual Prop. Section, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 104-07 (2002), available at http://www.usdoj.gov/criminal/cybercrime/ s&smanual2002.pdf (on file with the Columbia Law Review) [hereinafter DOJ Manual]. The manual notes that: Some providers retain records for months, others for hours, and others not at all. As a practical matter, this means that evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, agents may learn of a child pornography case on Day 1, begin work on a search warrant on Day 2, obtain the warrant on Day 5, and then learn that the network service provider deleted the records in the ordinary course of business on Day 3. Id. at 104-05.

[15] See Kerr, Internet Surveillance, supra note 10, at 616-18 (explaining distinction between prospective and retrospective surveillance).

[16] One early example of how such a trail of evidence might be traced back to a suspect is recounted in Cliff Stoll's The Cuckoo's Egg. See Cliff Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (1990).

على أن فريد ارتكب السرقة. وفي النسخة الرقمية من الجريمة، من المرجح likely أن تكون هذه الخطوة ضرورية. قد تظهر الأدلة الرقمية المأخوذة من الخوادم أن حسابا معينا قد استخدم لسرقة أموال من البنك، ولكنها لن تثبت أبدا أن شخصا معينا كان يتحكم في الحساب[17]. وهناك شيء مهم مفقود: بديل لشهادة شهود العيان البيومترية biometric eyewitness testimony أو الأدلة المادية physical evidence لربط الأدلة الموجودة بشخص معين. وبدون هذا الارتباط، لن تتمكن السلطات من إثبات القضية بما لا يدع مجالا للشك.

سيكون المفتاح في معظم الحالات هو استعادة الحاسوب المستخدم لشن الهجوم. فإذا تمكنت الشرطة من العثور على الحاسوب المنزلي الخاص بفريد وتحليله، فمن المحتمل أن تسفر عن أدلة دامغة. يمكن أن تسمح السجلات التي تحتفظ بها معظم أنظمة التشغيل لخبراء الطب الشرعي forensics experts بإعادة البناء بتفاصيل مدهشة من فعل ماذا ومتى[18]. وحتى الملفات المحذوفة deleted files يمكن استردادها في كثير من الأحيان[19]، كوظيفة حذف delete function عادة ما تشير فقط إلى مساحة التخزين على أنها متاحة للمواد الجديدة ولا تمحو أي شيء في الواقع. فقد يكشف تحليل الحاسوب عن ملف يحتوي على كلمة مرور البنك المستخدمة لإعداد الحساب غير المصرح به[20]. وقد يكشف عن سجلات من هذا الحساب، أو سجلات مأخوذة من بعض أجهزة الحاسوب الوسيطة. حتى إذا لم يتم العثور على مثل هذه المستندات، فقد يكون من الممكن معرفة ما إذا كان الهجوم قد تم إطلاقه من الحاسوب. يمكن أن يوفر هذا الدليل دليلا مقنعا على الإدانة. في حين قد توجد تفسيرات بريئة لسبب استخدام الحاسوب الشخصي للمشتبه به لشن هجوم، فإن ربط الهجوم بالممتلكات الخاصة للمشتبه به يمكن أن يقطع شوطا طويلا نحو القضاء على الشك المعقول.

لقد طور خبراء المعامل الشرعية الحاسوبية Computer forensics experts مجموعة مفصلة من الإجراءات التي يتبعها محللو الطب الشرعي عادة عند الاستيلاء على حاسوب الهدف وتحليله[21]. والتفاصيل الفنية ليست مهمة هنا، ولكن المخطط العام مهم. أولا، عادة ما يصادر المحققون الحاسوب ويعيدونه إلى مختبر المعمل الشرعي الحكومي لتحليله[22]. ويعتبر ذلك ضروريا لأن اجراءات المعمل الشرعي تستغرق وقتا طويلا. ولا يستطيع خبراء الحاسوب عادة العثور على الأدلة على القرص الصلب في الوقت الذي يسمح بإجراء البحث في الموقع[23]. وبالعودة إلى المعمل، يبدأ المحلل بإنشاء صورة "تدفق البتات bitstream" أو

[17] As the Justice Department has recognized, "generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it." See DOJ Manual, supra note 12, at 69.
[18] See Eric Friedberg, Catch as Cache Can: Forging or Altering Electronic Documents Leaves Tell-Tale Fingerprints Behind, Legal Times, Feb. 2, 2004, at 36.
[19] See, e.g., United States v. Upham, 168 F.3d 532, 533 (1st Cir. 1999).
[20] See James M. Rosenbaum, In Defense of the Delete Key, 3 Green Bag 2d 393, 393 (2000).
[21] See, e.g., United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997). In Whitaker, the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included a spreadsheet file detailing records of narcotics sales and amounts owed to him by his coconspirators. See id.
[22] See generally Bill Nelson et al., Guide to Computer Forensics and Investigations (2004) (surveying current computer forensics practices).
[23] See DOJ Manual, supra note 12, at 44 ("As a practical matter, circumstances will often require investigators to seize equipment and search its contents off-site.").

"مرأة انعكاس mirror" لمحرك الأقراص الثابتة[24]. ونسخة تدفق البتات هي نسخة مكررة تماما، ليس فقط من الملفات، ولكن من كل بت وبايت مخزن على محرك الأقراص[25]. ثم يقوم المحلل بعمله على النسخة بدلا من الأصل لضمان عدم تلف الأصل أو تغييره من خلال تحقيق المحلل[26].

وقد يجرب المحلل مجموعة من التقنيات لتحديد الأدلة المطلوبة. على سبيل المثال، قد يبدأ الفاحص بتنفيذ عمليات بحث سلسلة عن امتدادات extensions أو عبارات phrases أو أجزاء نصية textual fragments معينة تتعلق بالأدلة التي تبرر البحث. بدلا من ذلك، يجوز له فتح جميع الملفات ذات الخصائص الخاصة أو عينة من الملفات حتى يجد الأدلة التي تربط المشتبه به بالجريمة. وفي حالة فريد، على سبيل المثال، قد يبدأ المحقق بالبحث في القرص الصلب عن كلمة مرور البنك، أو ربما عن اسم البنك. إذا لم يفلح ذلك، فقد يبدأ المحقق في البحث عن تاريخ المستندات المختومة في يوم هجوم فريد، أو قد يبحث فقط عن أية مستندات مالية. وبمجرد أن يفهم كيف قام فريد بتخزين البيانات على محرك الأقراص الثابتة الخاص به، قد يجد المحقق قدرا كبيرا من المعلومات التي تدينه. بافتراض أن فريد لم يتم إبلاغه بالتحقيق ولم يمحو الملفات ذات الصلة بشكل دائم، فقد يجد المحلل كلمة المرور الرئيسية للبنك وسجلات الحساب والأدلة الأخرى التي تربط الحاسوب ومالكه بالجريمة.

لنفترض أن هذه التكتيكات ناجحة، وأن تحليل حاسوب فريد يكشف عن أدلة على الهجوم. فريد متهم، والقضية تذهب إلى المحاكمة. سيضع المدعي العام الشهود على المنصة بطريقة تتبع مسار التحقيق. أولا، سيدلي موظف البنك بشهادته حول الهجوم وخسائر البنك. وبعد ذلك، سيدلي مسؤولو نظام أجهزة الحاسوب الوسيطة بشهاداتهم حول ارتباطهم في سلسلة الأدلة، وسيدلي موظف من مزود خدمة الإنترنت الخاص بفريد بشهادته حول القرائن الإلكترونية electronic clues التي تؤدي إلى حساب فريد. وأخيرا، سيدلي عملاء الحكومة بشهاداتهم. سيشهد المحقق أنه استعاد الحاسوب داخل منزل فريد، وسيشهد خبير المعمل الشرعي للحاسوب أن حاسوب فريد يحتوي على أدلة على الهجوم مع ملفات فريد الشخصية. تثبت قضية الحكومة الآن بما لا يدع مجالا للشك أن فريد ارتكب سرقة البنك عبر الإنترنت.

[24] See United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant.").
[25] As the Justice Department has explained: Creating a duplicate copy of an entire drive (often known simply as "imaging") is different from making an electronic copy of individual files. When a computer file is saved to a storage disk, it is saved in randomly scattered sectors on the disk rather than in contiguous, consolidated blocks; when the file is retrieved, the scattered pieces are reassembled from the disk in the computer's memory and presented as a single file. Imaging the disk copies the entire disk exactly as it is, including all the scattered pieces of various files (as well as other data such as deleted file fragments). The image allows a computer technician to recreate (or "mount") the entire storage disk and have an exact copy just like the original. In contrast, a file-by-file copy (also known as a "logical file copy") merely creates a copy of an individual file by reassembling and then copying the scattered sectors of data associated with the particular file. DOJ Manual, supra note 12, at 42 n.6.
[26] See, e.g., United States v. Triumph Capital Group, 211 F.R.D. 31, 48 (D. Conn. 2002).

II. الدليل الرقمي وفشل القواعد النافذة

II. DIGITAL EVIDENCE AND THE FAILURE OF EXISTING RULES

قواعد الإجراءات الجنائية الحالية Existing rules of criminal procedure هي منتجات عضوية organic products مصممة بشكل طبيعي لوقائع التحقيقات في الجرائم المادية. إن مقارنة ملامح قواعد الإجراءات الجنائية الحالية بخطوات التحقيق الشائعة في مثل هذه التحقيقات التقليدية تكشف عن تطابق واضح. القواعد المعاصرة للإجراءات الجنائية هي قواعد العالم المادي التي تعكس حقائق تحقيقات العالم المادي. وهي تحاول تحقيق التوازن بين الخصوصية واحتياجات إنفاذ القانون في ضوء الحقائق المتعلقة بكيفية جمع الشرطة للأدلة المادية وشهادات شهود العيان[27].

ومع ذلك، فإن تطبيق المذهب الحالي على جمع الأدلة الرقمية يؤدي إلى بعض النتائج المذهلة. والقواعد التي تنظم بشكل معقول التحقيق في الجرائم المادية بناء على الوقائع المادية physical facts تؤدي إلى نتائج مفاجئة عند تطبيقها على التحقيقات الجديدة. ففي العديد من المراحل، تفرض هذه النتائج قيودا قليلة على التحقيقات الحكومية، إن وجدت. وفي مراحل قليلة، تفرض حواجز غير ضرورية أمام نجاح التحقيقات. حيث يوضح هذا الجزء كيف تعمل القواعد الحالية بشكل جيد وبشكل معقول في الحالات التقليدية، ولكنها غالبا ما تفشل في تنظيم جمع الأدلة الرقمية بشكل فعال.

A. جرائم العالم المادي وقواعد الاجراءات الجنائية

A. Physical Crimes and Rules of Criminal Procedure

من الطبيعي أن تصمم قواعد الإجراءات الجنائية القائمة وفقا لوقائع جرائم العالم المادي. اذ ضع في اعتبارك حظر التعديل الرابع لعمليات التفتيش والمصادرة غير المعقولة[28]. وتنظم قواعد التعديل الرابع بشأن "عمليات التفتيش searches" غير المعقولة unreasonable جمع الأدلة في شكل شهادة شهود عيان من قبل ضباط الشرطة. وتحكم قواعد التفتيش أين وفي أي ظروف يمكن لمأموري الضبط القضائي أن يذهبوا للإبلاغ عما تلاحظه حواسهم senses observe[29].

ومن خلال تنظيم الأماكن التي يمكن أن يذهب إليها الضباط/ مأمورو الضبط القضائي، تنظم قواعد التفتيش ما يراه هؤلاء ويسمعونه. ومن خلال تنظيم ما يرونه ويسمعونه، تحد القواعد من نطاق الأدلة التي يمكنهم جمعها. غالبا ما يتم حجب هذه الوظيفة من خلال سخرية المحكمة الشهيرة في قضية كاتز ضد الولايات المتحدة Katz v. United States بأن "التعديل الرابع يحمي الناس وليس الأماكن"[30].وكما أشار القاضي

[27] C.f. Nadine Strossen, The Fourth Amendment in the Balance: Accurately Setting the Scales Through the Least Intrusive Alternative Analysis, 63 N.Y.U. L. Rev. 1173, 1181-84 (1988) (describing the use of balancing tests in Fourth Amendment law).
[28] . U.S. Const. amend. IV.
[29] See William J. Stuntz, Reply, 93 Mich. L. Rev. 1102, 1102-03 (1995) [hereinafter Stuntz, Reply] (noting that "[t]he Fourth Amendment regulates street stops, but it pays little attention to how coercively the police behave in those stops-instead, the law concerns itself with whether and when the police can look in suspects' pockets").
[30] Katz v. United States, 389 U.S. 347, 351 (1967).

هارلان Justice Harlan في موافقته على كاتز، فإن مسألة الحماية التي توفرها للناس "تتطلب الإشارة إلى" مكان "place"[31].

وبموجب صياغة القاضي هارلان، يظل التعديل الرابع مرتبطا بشدة بالأماكن. في صياغة ويليام ستونتز William Stuntz، فإن القانون "ينظم ما يمكن لمأموري الضبط القضائي رؤيته وسماعه"، مع التركيز على المكان الذي يمكنهم الذهاب إليه أكثر مما يفعلونه بمجرد وصولهم إلى هناك[32].

وعلى وجه التحديد، تم تفسير اختبار كاتز "التوقع المعقول للخصوصية reasonable expectation of privacy" بطريقة تفصل بشكل فعال المساحات المادية العامة عن المساحات المادية الأكثر خصوصية[33]. ويمكن لمأمور الضبط القضائي دخول أية مساحة غير محمية بتوقع معقول للخصوصية. مثل هذا المدخل لا يعتبر "تفتيشا". ويسمح هذا لمأموري الضبط القضائي بالتجول في الشوارع العامة أو الأماكن الأخرى المفتوحة للجمهور دون قيود.

وفي المقابل، يمكن للضابط دخول المساحات المحمية بتوقع معقول للخصوصية فقط في ظل ظروف خاصة. ويشكل الدخول إلى حيز خاص مثل منزل أو مكتب تفتيشا، وهو معقول (وبالتالي دستوري) فقط إذا كانت تبرره ظروف خاصة[34]. وقد تشمل هذه الظروف الخاصة وجود أمر تفتيش صالح، أو موافقة شخص له سلطة مشتركة على المكان، أو وجود ظروف ملحة[35].

وبمجرد دخول المحقق بشكل شرعي إلى مساحة معينة، يكون حرا في الإدلاء بشهادته حول كل ما يلاحظه دون توريط التعديل الرابع[36]. ولا تحتاج الشرطة إلى "إبعاد أعينها عن الأدلة على النشاط الإجرامي"[37]. وأي شيء يراه الضابط هو "على مرأى من الجميع plain view"[38]، أي شيء يشمه هو رائحة عادية[39]، وأي شيء يسمعه غير محمي بموجب التعديل الرابع[40].

في حين أن قواعد التفتيش تنظم مجموعة شهادات شهود العيان من قبل ضباط الشرطة the search rules regulate the collection of eyewitness testimony by police officers، فإن قواعد الضبط/ المصادرة تحكم جمع الأدلة المادية the seizure rules govern the collection of physical evidence. عرفت المحكمة العليا "ضبط "seizure الممتلكات بأنه "تدخل ذي مغزى في مصالح حيازة

[31] Id. at 361 (Harlan, J., concurring)
[32] Stuntz, Reply, supra note 28, at 1102. Stuntz goes on to note that "the law limits police officers' ability to enter people's houses but turns a blind eye to how violently the cops behave once inside." Id. at 1103.
[33] For a discussion of how the "reasonable expectation of privacy" test applies to investigative steps involving technologies that can conduct searches without invading physical space, see Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 827-837 (2004) [hereinafter Kerr, New Technologies].
[34] Illinois v. Andreas, 463 U.S. 765, 771 (1983)
[35] Smith v. Maryland, 442 U.S. 735, 739-40 (1979).
[36] Illinois v. Rodriguez, 497 U.S. 177, 183-84 (1990).
[37] But see Harold J. Krent, Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment, 74 Tex. L. Rev. 49, 51 (1995) (arguing that Fourth Amendment should be interpreted to provide use restrictions on information gathered by government).
[38] California v. Greenwood, 486 U.S. 35, 41 (1988).
[39] Horton v. California, 496 U.S. 128, 135 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 465-66 (1971) (Stewart, J., concurring)).
[40] United States v. McCoy, 200 F.3d 582, 584 (8th Cir. 2000).

الفرد في تلك الممتلكات meaningful interference with an individual's possessory interests in that property "[41]. وبموجب هذا الاختبار، يعد جمع الأدلة المادية بمثابة ضبط seizure. وتشرح حالات التعديل الرابع متى تكون هذه المضبوطات معقولة، وبالتالي مسموح بها allowable. وعادة ما تكون المضبوطات القصيرة جدا التي تتم لأغراض إنفاذ القانون المشروعة legitimate law enforcement purposes معقولة، ولكن المضبوطات الممتدة extended seizures عادة ما تكون غير معقولة unreasonable ما لم تحصل الشرطة على أمر قضائي warrant [42]. وعادة ما تكون المضبوطات التي لا تتعدى مباشرة على المصالح الحيازية معقولة؛ على سبيل المثال، يمكن للمحقق أن يأخذ الأدلة إذا وافق مالكها owner consents [43]، أو إذا تم التخلي عن الأدلة[44].

كما تنظم الأحكام الدستورية التي تتجاوز التعديل الرابع خطوات التحقيق التقليدية. ينص التعديل الخامس على أنه "لا يجوز إجبار أي شخص في أية قضية جنائية على أن يكون شاهدا ضد نفسه"[45]. ,هذا الحق في عدم تجريم الذات يحد من جمع شهادات شهود العيان من خلال تنظيم متى يمكن للمحققين استخدام الأقوال ضد المتهم. وبالمثل، يضمن التعديل السادس لكل متهم "عملية إلزامية للحصول على شهود لصالحه"[46]، مما يمكن المتهم من جمع شهادات شهود العيان الخاصة به. وتركز كلتا المجموعتين من القواعد على تحقيق التوازن بين حقوق الحكومة والمتهم في التحقيقات التقليدية في الجرائم التقليدية.

يمكننا أن نرى كيف تعمل القواعد التقليدية للإجراءات الجنائية في الممارسة العملية من خلال إعادة النظر في التحقيق في سرقة بنك فريد المادية. المحقق حر في فحص الجزء الخارجي من البنك: لا يوجد توقع معقول للخصوصية في ما يتعرض للجمهور[47]. ويمكنه دخول البنك خلال ساعات العمل للنظر حوله أيضا. نظرا لأن البنك مفتوح للجمهور، فإن دخول البنك ليس تفتيشا. إذا أراد أن ينظر عن كثب إلى البنك بعد ساعات، فإنه يحتاج إلى موافقة موظف البنك.

الارادة Consent ستجعل التفتيش معقولا، وبالتالي مسموحا به دستوريا. يمكن للمحقق أيضا التحدث مع شهود العيان وتسجيل ملاحظاتهم على الجريمة. إذا وجد المحقق مسدس فريد فيلوني، فيمكنه ضبطه seize:

الضبط معقول seizure is reasonable بموجب التعديل الرابع طالما أن فائدة البندقية كدليل واضحة على الفور[48]. ومع ذلك، إذا صادف أدلة أخرى لا علاقة واضحة لها بالجريمة، فلا يمكنه عادة ضبطها. إذا اختارت

[41] Abel v. United States, 362 U.S. 217, 241 (1960) (holding that it is lawful for government investigators to seize abandoned property).
[42] Schneckloth v. Bustamonte, 412 U.S. 218, 219-20 (1973).
[43] United States v. Place, 462 U.S. 696, 701 (1983) (noting that in "the ordinary case," seizures of personal property are "unreasonable within the meaning of the Fourth Amendment unless . .. accomplished pursuant to a judicial warrant," issued after finding probable cause). Schneckloth v. Bustamonte, 412 U.S. 218, 219-20 (1973).
[44] Abel v. United States, 362 U.S. 217, 241 (1960) (holding that it is lawful for government investigators to seize abandoned property).
[45] U.S. Const. amend. V. The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself."
[46] Id. amend. VI the Sixth Amendment guarantees every defendant "compulsory process for obtaining witnesses in his favor,".
[47] See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (noting that what is exposed to the public cannot receive Fourth Amendment protection).
[48] Horton v. California, 496 U.S. 128, 136 (1990) (citing Coolidge v. New Hampshire, 403 U.S. 443, 466 (Stewart, J., concurring) (1971)).

الشرطة تفتيش منزل فريد بحثا عن أدلة، فستحتاج إلى أذن تفتيش warrant لتبرير دخوله إلى مساحته الخاصة private space[49].

تضمن قواعد التعديل الرابع التي تحكم أوامر التفتيش أن يكون التفتيش مصمما بشكل ضيق narrowly tailored: يجب أن يقتصر على المكان المادي المحدد حيث من المحتمل أن تكون الأدلة موجودة ويجب أن يقتصر التفتيش على عناصر محددة مرتبطة بسرقة البنك[50]. ثم يكون المحقق حرا في الإدلاء بشهادته حول كل ما لاحظه أثناء التحقيق. وتنظم قواعد الإجراءات الجنائية القائمة مجتمعة بشكل فعال جمع الأدلة المادية وشهادات شهود العيان.

B. الأدلة الرقمية وقواعد العالم المادي

B. Digital Evidence and Physical-World Rules

تتغير الصورة بشكل كبير عندما ننتقل من التحقيقات التقليدية التي تنطوي على شهادة شهود العيان والأدلة المادية إلى التحقيقات التي تتطلب جمع الأدلة الرقمية digital evidence. كما ذكرنا سابقا، هناك ثلاث آليات أساسية لجمع الأدلة الرقمية three basic mechanisms of digital evidence collection: جمع الأدلة المخزنة من أطراف ثالثة third parties، وجمع الأدلة المخزنة من الهدف target، وجمع الأدلة أثناء النقل in transit. ويكشف تطبيق المذاهب القائمة على هذه الآليات الثلاث عن عدة صعوبات.

تميل القواعد التقليدية إلى عدم ترجمة الحقائق الجديدة بشكل جيد. هناك ما يبرر الحذر: من المثير للدهشة وجود عدد قليل من الحالات التي تطبق العقيدة التقليدية على جمع الأدلة الرقمية. يتطلب ربط القواعد القديمة بالحقائق الجديدة بعض التكهنات. وفي الوقت نفسه، تظهر المقارنة بين الخطوط الأساسية للقانون الحالي والديناميكيات المشتركة في قضايا الأدلة الرقمية ضعف التوافق بينهما. وفي كثير من الظروف، لا توفر القواعد التقليدية أي حد حقيقي لممارسات إنفاذ القانون. في ظروف أخرى، تسمح لتهديدات الخصوصية الوهمية بمنع خطوات التحقيق الضرورية.

1. **الأدلة من أطراف ثالثة وعملية الاستدعاء.** ان النظر في المرحلة الأولى من معظم التحقيقات في الجرائم الإلكترونية، حيث يتصل المحققون بمديري النظام ويحصلون على الأدلة المخزنة المتعلقة بالجريمة من الخوادم المستخدمة في سياق الجريمة[51]. وتثير هذه العملية شواغل هامة تتعلق بالخصوصية مما يشير إلى الحاجة إلى تنظيم قانوني دقيق careful legal regulation. يقوم مستخدمو الإنترنت بشكل روتيني بتخزين معظم معلوماتهم الخاصة إن لم يكن كلها على خوادم بعيدة remote servers، وكل هذه المعلومات متاحة لمسؤولي النظام[52]. ويمكن لمديري النظام System administrators قراءة البريد الإلكتروني الخاص، والتفتيش في الملفات المخزنة، والوصول إلى سجلات الحسابات التي تسجل كيفية استخدام المشتركين الافراد

[49] Kyllo v. United States, 533 U.S. 27, 40 (2001).
[50] See, e.g., Horton, 496 U.S. at 138-40; United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) (noting that probable cause to seize specific paper files enumerated in warrant does not permit seizure of commingled innocent files).
[51] See supra notes 8-11 and accompanying text.
[52] See, e.g., Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1092-94 (2002) (discussing information stored by service providers).

للشبكة. نتيجة لذلك، يمكن أن تكون القدرة على إجبار compel مزودي خدمة الإنترنت للإفصاح على الادلة هي القدرة على إجبار الكشف عن عالم المستخدم عبر الإنترنت بالكامل. بالإضافة إلى ذلك، يمكن أن يحدث الإفصاح دون إشعار المستخدم، ويمكن أن يتضمن حسابات متعددة. يمكن أن تكون القدرة على إجبار الأدلة من مزودي خدمة الإنترنت هي القدرة على الكشف عن الملف الشخصي عبر الإنترنت لمئات أو حتى آلاف المستخدمين في وقت واحد، وكل ذلك في سرية تامة in total secrecy.

ومن اللافت للنظر أن مبدأ التعديل الرابع والخامس الحالي لا يوفر أية حماية خصوصية لتنظيم هذه العملية. ويمكن للمحققين إجبار مسؤولي النظام على الكشف عن المعلومات المخزنة في خوادمهم باستخدام مذكرات الاستدعاء subpoenas [53]. ويتم تنظيم مذكرات الاستدعاء بشكل طفيف بموجب التعديل الرابع: يتطلب القانون الحالي فقط أن تكون المعلومات أو الممتلكات التي سيتم الاجبار فيها ذات صلة بالتحقيق، وأن إنتاجها يجب ألا يكون عبئا مفرطا على متلقي أمر الاستدعاء[54]. ويغطي معيار الصلة كل شيء تقريبا، لأنه يشمل مجرد التحقق للتأكد من عدم ارتكاب أي جريمة[55]. حدود العبء هي بالمثل بلا أسنان في سياق الأدلة الإلكترونية electronic evidence:

ومن السهل عموما على مزود خدمة الإنترنت أن ينسخ الملفات الضخمة voluminous files ويعطيها للمحققين[56]. وغالبا ما يجد مزودو خدمات الإنترنت أنه من الأسهل تسليم المعلومات بشكل جماعي بدلا من التصفية بشق الأنفس من خلال الملفات لتحديد الملف المطلوب بدقة[57]. ولا يلزم إبلاغ الشخص قيد التحقيق بوجود أمر الاستدعاء[58]. ولا ينطبق امتياز التعديل الخامس لأن متلقي أمر الاستدعاء هو طرف ثالث بريء[59]. وفي ضوء هذه الحقائق، إن تطبيق قواعد التعديل الرابع والخامس التقليدية على جرائم الشبكة الجديدة يترك المرحلة الأولى من التحقيقات في جرائم الشبكة غير منظمة بالكامل تقريبا.

كيف يمكن للقانون أن يسمح بمثل هذه النتيجة المذهلة؟ يكمن التفسير في التحول من الدور الذي تلعبه مجموعة أدلة الطرف الثالث في التحقيقات التقليدية إلى الدور الذي تلعبه في قضايا الأدلة الرقمية. في الماضي، لعب

---

[53] The two most common types of subpoenas track the traditional evidence gathering techniques in physical-world crimes. They are subpoenas ad testificandum, subpoenas to testify before a grand jury, and subpoenas duces tecum, subpoenas ordering the recipient to give physical evidence to the grand jury. See Black's Law Dictionary 1467 (8th ed. 2004).

[54] See United States v. Dionisio, 410 U.S. 1, 10 (1973) (noting that forcing compliance with a grand jury subpoena raises minimal privacy concerns).

[55] See United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950) (noting that a grand jury subpoena can be issued even just to make sure that no crime has been committed).

[56] Cf. William J. Stuntz, Commentary, O.J. Simpson, Bill Clinton, and the Trans substantive Fourth Amendment, 114 Harv. L. Rev. 842, 857-58 (2001) [hereinafter Stuntz, Commentary] ("While searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.").

[57] In my experience working with ISPs in digital evidence investigations, system administrators occasionally expressed willingness to turn over many gigabytes of information relating to thousands of customers rather than go through the trouble of searching through their files for the documents relating to the target of the investigation.

[58] See SEC v. O'Brien, Inc., 467 U.S. 735, 743 (1984) (rejecting arguments that a suspect is entitled to notice of a third-party administrative subpoena).

[59] See Fisher v. United States, 425 U.S. 391, 397 (1976) (holding that Fifth Amendment privilege does not immunize third-party agent from complying with subpoena directed to suspect's information in the agent's possession).

جمع أدلة الطرف الثالث دورا ضيقا ولكنه مهم ينطوي على الخصوصية بطرق محدودة نسبيا. الدور ضيق لأن مرتكبي الجرائم المادية يحتفظون عموما بالأدلة لأنفسهم بدلا من إعطائها لأطراف ثالثة. إذا سرق فريد فيلوني بنكا، فسيحتفظ بالمسروقات ويخزن أدواته في مكان آمن. من غير المحتمل أن يشارك أدلة الإدانة مع أشخاص لا يعرفهم.

وفي هذا السياق، تشكل سلطة الاستدعاء تهديدا صغيرا نسبيا بتجاوز الحكومة الغازية. إذا اشتبه ضابط شرطة في أن فريد فوني هو سارق البنك، فلا يمكنه ببساطة إصدار أمر استدعاء يأمر فريد بتسليم أي دليل أو ثمار الجريمة. ومن الناحية العملية، فانه من غير المرجح أن يمتثل فريد، وإصدار أمر الاستدعاء سيرشده إلى التحقيق. كمسألة قانونية، سيتمتع فريد بامتياز التعديل الخامس لرفض الامتثال لأمر الاستدعاء. ولأن الامتثال سيظهر العلم بالمسروقات وحيازتها، فإن الامتياز ضد تجريم الذات self-incrimination سيجعل أمر الاستدعاء باطلا قانونيا[60].

تخدم مذكرات الاستدعاء غرضا مهما في مجموعة محددة من القضايا التقليدية: فهي ضرورية في التحقيقات المكثفة في جرائم ذوي الياقات البيضاء white-collar crime.

كما لاحظ ويليام ستونتز William Stuntz، يمكن فهم الحماية الضعيفة weak protections التي تنظم سلطة الاستدعاء جزئيا على الأقل على أنها نتاج طارئ لتاريخ التعديل الرابع[61]. وفي القضية المبكرة لبويد ضد الولايات المتحدة Boyd v. United States، رأت المحكمة العليا أن الأمر بفرض الكشف عن الأدلة يجب أن ينظم بعناية مثل التفتيش المباشر direct search أي قيام مأمور الضبط بطرق الباب[62]. حيث تراجعت المحكمة عن هذا المعيار بعد عشرين عاما في قضية هيل ضد هانكل Hale v. Henkel. ومع ذلك، عندما استبدلت بويد Boyd بعتبة الدرج المنخفضة low threshold التي استوفت أمر الاستدعاء وفق التعديل الرابع طالما أنه لم يكن "مكتسحا sweeping"[63].

واليوم، لا يزال القانون مشابها تقريبا للقانون الذي أعلن عنه قبل قرن من الزمان في قضية هانكل Henkel[64]. ولماذا التغيير؟ فقد شهد المناخ التنظيمي regulatory climate في أواخر القرن التاسع عشر وأوائل القرن العشرين صعود التحقيقات في جرائم ذوي الياقات البيضاء white-collar crime investigations، وطالبت تلك التحقيقات بسهولة الوصول إلى الوثائق التي يمكن أن تثبت ارتكاب

[60] United States v. Hubbell, 530 U.S. 27, 36-37 (2000). Even beyond these practical concerns, there are the very different ways in which subpoenas and direct searches pursuant to warrants are executed. Consider Judge Henry Friendly's rationale for why the Fourth Amendment offers little regulation of subpoenas. He looked to the physical mechanism of how the orders are executed: The [direct search] is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court. United States v. Doe, 457 F.2d 895, 898 (2d Cir. 1972).

[61] See Stuntz, Commentary, supra note 57, at 857-59.

[62] 116 U.S. 616, 630 (1886). Boyd involved an order to disclose customs invoices. The Court suggested that there was no Fourth Amendment difference between a direct search and an order to disclose: Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods, is within the condemnation of [the Fourth Amendment]. Id.

[63] 201 U.S. 43, 76 (1906).

[64] See United States v. Dionisio, 410 U.S. 1, 11 (1973) (affirming the rule of Hale).

مخالفات[65]. كما أوضح ستونتز Stuntz، **"إن معيار السبب المحتمل لمذكرات الاستدعاء من شأنه أن ينهي العديد من التحقيقات الجنائية لأصحاب الياقات البيضاء قبل أن تبدأ"**[66]. إن الجمع بين الدور الأساسي لمذكرات الاستدعاء في فئة ضيقة من القضايا التي تتطلب وثائق مكثفة والتهديد المحدود عموما للخصوصية في أماكن أخرى قد تظافر لخلق بيئة لا يتم فيها تنظيم عملية الاستدعاء إلا بشكل خفيف للغاية.

ومع ذلك، فإن تساهل قاعدة الاستدعاء lax subpoena rule لا معنى لها بالنسبة للتحقيقات في جرائم شبكات الحاسوب computer-network crime investigations. غالبا ما يقوم مستخدمو الحاسوب بتخزين الكثير من معلوماتهم مع خوادم تابعة لجهات خارجية. إنها الطريقة التي تعمل بها الإنترنت. ويشير تطبيق القاعدة التقليدية على الحقائق الجديدة إلى أنه يمكن استدعاء عالم الإنترنت بأكمله من اتصالات الإنترنت المخزنة stored internet communications عبر وسطاء مزودي خدمة الإنترنت the intermediaries of ISPs. فلا التعديل الرابع ولا التعديل الخامس يوفر الكثير من الحماية.

ان التعديل الرابع لا يفعل الكثير لأن قواعد الخصوصية الخاصة به ضعيفة للغاية، والتعديل الخامس يفشل لأن الأطراف الثالثة مثل مزودي خدمة الإنترنت يمكنهم الكشف عن المعلومات دون توريط أي امتياز ضد تجريم الذات self-incrimination من تلقاء أنفسهم[67]. في حين أن سلطة الاستدعاء subpoena power ضيقة إلى حد ما في القضايا التقليدية، وفي قضايا جرائم الحاسوب فهي واسعة بشكل لا يصدق. وبالنسبة للمحققين، فإن إجبار مزود خدمة الإنترنت على الكشف عن المعلومات أفضل من بديل التفتيش من خلال خادم مزود خدمة الإنترنت مباشرة: حيث يمكن للموظفين ببساطة إرسال نسخة من أمر الاستدعاء بالفاكس إلى مقر مزود خدمة الإنترنت وانتظار الطرد package أو إعادة الفاكس مع الوثائق ذات الصلة[68]. ولا يلزم وجود خبرة تقنية أو السفر إلى مزود خدمة الإنترنت.

تتحول القاعدة المعقولة reasonable rule التي تم تطويرها استجابة لحقائق تحقيقات العالم المادي إلى قاعدة غير معقولة وغير متوازنة عند تطبيقها على الحقائق الجديدة للتحقيقات في الجرائم الرقمية digital crime investigations.

2. المراقبة المستقبلية ومشكلة المراقبة بالتصنت.

2. Prospective Surveillance and the Problem of Wiretapping.

نواجه مشاكل مماثلة عندما يقوم المحققون بمراقبة مستقبلية من خلال مراقبة تدفق حركة المرور على الإنترنت[69]. حيث يمكن أن تكون المراقبة المستقبلية واسعة أو ضيقة، اعتمادا على المعلومات التي يسعى

[65] See Stuntz, Commentary, supra note 57, at 859.
[66] "a probable cause standard for subpoenas would end many white-collar criminal investigations before they had begun." Id. at 860. Stuntz continues: "In short, if the government is to regulate business and political affairs-the usual stuff of white-collar criminal law-it must have the power to subpoena witnesses and documents before it knows whether those witnesses and documents will yield incriminating evidence." Id.
[67] Fisher v. United States, 425 U.S. 391, 398-99 (1976) (holding that the Fifth Amendment does not regulate a subpoena served on tax preparer for tax documents given to the preparer by customers).
[68] United States v. Bach, 310 F.3d 1063, 1067-68 (8th Cir. 2002) (holding that such a procedure pursuant to a warrant does not violate the Fourth Amendment).
[69] Prospective surveillance can occur in the context of any computer network, and is not limited to cases involving the internet and internet packets. For the sake of simplicity, however, I will focus on the case of prospective surveillance involving packetized internet traffic.

إليها المحققون. ومع ذلك، فإن خطوة التحقيق الأساسية هي نفسها في كل حالة: يكمن الاختلاف الوحيد بين المراقبة الواسعة والضيقة في كيفية تكوين الفلتر.

وهذا صحيح لأن الإنترنت تعمل عن طريق خلط المعلومات معا أثناء الإرسال، وتكليف أجهزة الحاسوب tasking computers التي تتلقى المعلومات بإعادة تجميعها[70]. اذ يمكن أن تكون الأصفار وتلك التي تمر عبر كابل معين في وقت معين أي جزء من رسالة خاصة جدا، الصفحة الأولى من NYTimes.com، صورة للمواد الإباحية، أمر المتسلل إلى خادم بعيد، أو حركة مرور شبكة حاسوب إلى حاسوب لا معنى لها بشكل عام. حيث يحدد إعداد الفلتر/ مرشح المعلومات التي تم جمعها، مع إعداد مفتوح يؤدي إلى مراقبة كاملة وإعداد متقدم ينظم بإحكام نوع وكمية المعلومات التي تم جمعها.

وعلى الرغم من عدم تطبيق أية محكمة للتعديل الرابع على هذه الحقائق الدقيقة، إلا أن العقيدة الحالية تبدو غير مجهزة بشكل جيد لتنظيم المراقبة المحتملة. ومن وجهة نظر السياسة العامة standpoint of policy، قد تسمح القاعدة المعقولة sensible rule لضباط الشرطة police officers بجمع المعلومات التي تميل إلى أن تكون أقل خصوصية في ظل قواعد مخففة نسبيا، ولكنها تتطلب سلطة أكبر مثل أمر تفتيش search warrant للسماح بجمع المزيد من المعلومات الخاصة. اذ سوف تتوقف العتبة القانونية على إعداد الفلتر/المرشح، وربط درجة حماية الخصوصية بغزو المراقبة. إذا أراد المحققون فقط تحديد عنوان بروتوكول الانترنت IP الأصلي لاتصال معين، فيجب فرض عتبة منخفضة؛ إذا رغب المحققون في مراقبة مراسلات البريد الإلكتروني الخاصة، فيجب أن يفرض القانون عتبة عالية.

إن توليد مثل هذه القاعدة من عقيدة التعديل الرابع يثبت أنه صعب بشكل مدهش. المشكلة الأولى هي أن قواعد التعديل الرابع تركز تقليديا على مبرر الدخول إلى المساحة، وليس ما إذا كان العنصر الذي سيتم الاستيلاء عليه بعد دخول المساحة يجب اعتباره عاما أو خاصا.

حيث يحتاج مأمور الضبط القضائي إلى أمر لدخول منزلك بغض النظر عما إذا كانوا يخططون لقراءة مذكراتك الشخصية أو يريدون فقط رؤية صحيفة الصباح واقتحام break لقراءة نسختك[71]. وبالمثل، لا تحتاج الشرطة إلى أمر لجمع وتحليل وثائقك الخاصة المتروكة في حديقة عامة[72]." فالتركيز التقليدي على الدخول إلى المساحة منطقي للتحقيقات المادية. وفي العالم المادي، يحدد تنظيم المكان الذي يذهب إليه مأمور الضبط بما سيراه ويشمه ويسمعه ويشعر به. ستسجل الحواس البشرية للضابط الملاحظات التي يمكن لمأمور الضبط تذكرها لاحقا والإدلاء بشهادته في المحكمة. وبالتالي فإن تنظيم الدخول يعمل كطريقة وظيفية لتنظيم جمع الأدلة[73]. ويفصل اختبار "التوقع المعقول للخصوصية reasonable expectation of privacy"

[70] See Vincenzo Medillo et al., A Guide to TCP/IP Internetworking (1996), at http://www.ictp.trieste.it/~radionet/nucl996/ref/tcpip/partl.htm (on file with the Columbia Law Review) (describing the internet as transmitting separate packets of data)

[71] See Soldal v. Cook County, 506 U.S. 56, 69 (1992) ("[T]he reason why an officer might enter a house or effectuate a seizure is wholly irrelevant to the threshold question whether the Amendment applies. What matters is the intrusion on the people's security from governmental interference."); cf. Arizona v. Hicks, 480 U.S. 321, 325 (1987) ("It matters not that the search uncovered nothing of any great personal value to respondent . . . . A search is a search, even if it happens to disclose nothing [of importance].").

[72] See Vincenzo Medillo et al., A Guide to TCP/IP Internetworking (1996), at http://www.ictp.trieste.it/~radionet/nucl996/ref/tcpip/partl.htm (on file with the Columbia Law Review) (describing the internet as transmitting separate packets of data).

[73] See Soldal v. Cook County, 506 U.S. 56, 69 (1992) ("[T]he reason why an officer might enter a house or effectuate a seizure is wholly irrelevant to the threshold question whether the Amendment applies. What

العام عن الخاص، ويقصر الملاحظة على المساحات العامة public spaces في غياب أسباب خاصة تبرر الدخول إلى المساحات الخاصة private spaces.

هذا التركيز لا معنى له عند تطبيقه على المراقبة المحتملة. حيث يحدث الدخول إلى الخط المستغل لحركة المرور على الإنترنت internet traffic بغض النظر عما إذا كانت المراقبة ضيقة للغاية أو واسعة بشكل مذهل. وبدلا من أن يمثل الدخول تجاوزا للخط الفاصل بين العام والخاص، أصبح الآن مجرد شرط مسبق لأي جمع للأدلة. ومن غير الواضح حاليا ما إذا كان لدى مستخدمي الإنترنت توقع معقول للخصوصية في اتصالاتهم عبر الإنترنت، وبالتالي ما إذا كان ينبغي اعتبار الأسلاك التي تحتوي على حركة مرور الإنترنت مساحة خاصة أو عامة لأغراض التعديل الرابع[74]. كما أوضحت في مكان آخر، توجد حجج مهمة لكلا الموقفين[75].

ولكن في كلتا الحالتين، لن ترتبط القاعدة القانونية الناتجة عن ذلك بغزو invasiveness ممارسة المراقبة ذات الصلة. فإذا نظرت المحاكم إلى حركة المرور السلكية على الإنترنت على أنها أماكن عامة لا يمكن للأفراد فيها الاحتفاظ بتوقع معقول للخصوصية، فلن تفرض القواعد التقليدية أي قيود دستورية على المراقبة المحتملة[76]. وإذا فسرت المحاكم هذه المساحات على أنها مساحات خاصة تدعم توقعا معقولا للخصوصية، فإن المراقبة المصممة لاستهداف حتى المعلومات غير السرية ستتطلب مع ذلك تبريرا قانونيا قويا[77]. لا تتطابق أي من القاعدتين مع المفاهيم البديهية intuitive notions حول كيفية فصل القانون بين العام والخاص.

تبقى المشكلة الأساسية حتى لو تجاوزت المحاكم هذه الصعوبة وحاولت حماية المواد الخاصة بشكل مباشر أكثر. تخيل أن المحاكم توقف نطاق حماية التعديل الرابع على ما إذا كانت المعلومات المعينة التي تم جمعها

---

matters is the intrusion on the people's security from governmental interference."); cf. Arizona v. Hicks, 480 U.S. 321, 325 (1987) ("It matters not that the search uncovered nothing of any great personal value to respondent . . . . A search is a search, even if it happens to disclose nothing [of importance].").

[74] See Kerr, Internet Surveillance, supra note 10, at 629 (noting possibility that courts may not find Fourth Amendment protection for internet communications).

[75] See Amicus Curiae Brief of Professor Orin Kerr in Support of the Appellant at 6-8, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), available at 2002 WL 32139374 (explaining that courts may view information transmitted across the internet either as equivalent of stored postal mail, in which case it is entitled to Fourth Amendment protection, or as equivalent of information disclosed to a third party, in which case it is not).

[76] See Kerr, Internet Surveillance, supra note 10, at 629 (noting possibility that courts may not find Fourth Amendment protection for internet communications)

See Amicus Curiae Brief of Professor Orin Kerr in Support of the Appellant at 6-8, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), available at 2002 WL 32139374 (explaining that courts may view information transmitted across the internet either as equivalent of stored postal mail, in which case it is entitled to Fourth Amendment protection, or as equivalent of information disclosed to a third party, in which case it is not).

[77] Cf. Berger v. New York, 388 U.S. 41, 58-60 (1967) (applying the Fourth Amendment to a wire communication in context of a wiretap). Berger addressed a facial challenge to a state wiretap statute, making it difficult to apply its principles to an asapplied factual context. At the same time, Berger does suggest that the act of wiretapping rather than the precise information collected is the core constitutional concern.

تبدو عامة أو أكثر خصوصية. في حين أن هذا يبدو معقولا من الناحية النظرية، إلا أنه من الصعب جدا تحقيقه في الممارسة العملية.

توفر التكنولوجيا العقبة الأولى. يمكن لمرشحات المراقبة الحالية تحديد أنواع حركة المرور، مثل الفرق بين البريد الإلكتروني وصفحة الويب. ويمكن للفلاتر تحديد كلمات معينة، أو تسجيل الاتصالات من أو إلى عناوين إنترنت معينة. ولكن لا يمكن لأي فلتر/ مرشح أن يصدر حكما مستنيرا حول ما إذا كانت مجموعة معينة من الأصفار والآحاد عامة أم خاصة. الصعوبة ليست فقط التكنولوجيا، ولكن حدود الخصم:

عادة لا تشير المراسلات إلى من أو ما الذي أرسلها أو استلمها، أو السياق الذي تم إرسالها أو استلامها فيه. وبدون هذه المعلومات، فانه من الصعب معرفة ما إذا كانت أصفار وأخرى معينة جزءا من اتصال قد يحميه التعديل الرابع في بيئة مادية مماثلة. تحل بنية العالم المادي هذه المشكلة في الحالات التقليدية عن طريق ترسيم الأماكن العامة عن الأماكن الخاصة. الشيء نفسه ينطبق على التنصت التقليدي عبر خطوط الهاتف. عند النقر على خط الهاتف يعترض بالضرورة مكالمة من إنسان إلى إنسان، فإن خط الهاتف يشبه كشك خاص افتراضي[78]. وكل شيء على الخط خاص. ومع ذلك، في حالة المراقبة المرتقبة للاتصالات عبر الإنترنت، يتم خلط القطاعين العام والخاص معا. فلا توجد طريقة واضحة للحصول على السياق اللازم لرسم خطوط التعديل الرابع التقليدية.

3. تفتيش جهاز الحاسوب الخاص بالهدف وقواعد الأمر.

3. Searching the Target's Computer and the Warrant Rules.

تكشف المرحلة الأخيرة من التحقيقات في جرائم الحاسوب عن مشاكل عميقة بشكل خاص تتعلق بالملاءمة بين القواعد التقليدية والوقائع الجديدة. وفي هذه المرحلة، يقوم مأمور الضبط القضائي بمصادرة الحاسوب الشخصي للمشتبه به ثم تحليله. ومن الواضح أن الأمر مطلوب لدخول المنزل والاستيلاء على ممتلكات المشتبه به[79]. ولكن إلى أي مدى يحد الأمر فعليا مما يمكن لمأمور الضبط القيام به؟ وفي الحالات التقليدية، تكفل القواعد التي تحكم عملية الأمر أن يظل التفتيش والمصادرة ضيقين نسبيا. حيث يجب أن يذكر الأمر كلا من المكان المحدد الذي سيتم تفتيشه والأدلة المحددة التي سيتم الاستيلاء عليها[80]. ويجب أن يقتصر الحجز على الأدلة الموصوفة في الأمر- والتي هي نفسها محدودة بنطاق السبب المحتمل للاعتقاد بأن الأدلة موجودة في المبنى- بالإضافة إلى الأدلة الأخرى التي تم اكتشافها على مرأى من الجميع أثناء التفتيش. وتساعد هذه القواعد على ضمان عدم تحول عمليات التفتيش إلى أوامر عامة التي تسمح بالتفتيش العام في ممتلكات المشتبه فيه[81].

---

[78] See Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronic recording of a conversation in a telephone booth falls within the Fourth Amendment's scope); Berger, 388 U.S. at 64 (describing wiretapping as akin to "a trespassory invasion of the home or office"); Olmstead v. United States, 277 U.S. 438, 475-76 (1928) (Brandeis, J., dissenting) ("Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard.").

[79] See Kyllo v. United States, 533 U.S. 27, 31 (2001) (noting that "[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no").

[80] See, e.g., Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[81] See id.

ومع ذلك، فإن تطبيق هذه القواعد على الأدلة الرقمية يضع سلسلة من الألغاز. ضع في اعتبارك الخطوة الأولى من اجراء الضبط seizure process، حيث يأخذ المحققون جهاز الحاسوب الخاص بالمتهم خارج الموقع لاختبار المعمل الشرعي. ويعد ضبط الحاسوب بالكامل ضروريا لأسباب عملية، ولكن قد يكون من الصعب تبريره بناء على القواعد التقليدية. وفي كثير من الحالات، تكون أجهزة الحاسوب مجرد جهاز تخزين للأدلة بدلا من الأدلة نفسها.

الدليل هو الملف الإلكتروني electronic file الذي تبحث عنه الشرطة والذي يصادف تخزينه مع العديد من الملفات غير الضارة داخل حاوية أجهزة الحاسوب[82]. وبموجب القواعد التقليدية، إذن، يبدو ضبط أجهزة الحاسوب للحصول على حفنة من الملفات أمرا فضفاضا appear to be overbroad[83]. فهو مشابه تقريبا لضبط منزل بأكمله وسحب محتوياته للتنقيب عنها تفتيشا عن أدلة على الجريمة، الذي يحظره التعديل الرابع[84]. والمشكلة هي أن القاعدة التقليدية تتطلب مستوى من الدقة الجراحية level of surgical precision والخبرة الممكنة للأدلة المادية ولكن ليس الأدلة الرقمية. فعندما سرق فريد فوني البنك ماديا، تمكنت الشرطة من الحصول على أمر بتفتيش منزله بحثا عن الفواتير المسروقة وتفتيش المنزل في غضون ساعات قليلة[85].

لم تكن هناك حاجة لسحب كل شيء في المنزل والبحث عنه بعد أسابيع أو حتى أشهر في المختبر. القاعدة التي تتطلب من الضبط القضائي البحث عن الفواتير واسترجاع الفواتير المذكورة في الأمر فقط هي قاعدة معقولة في مثل هذه البيئة. ان تفتيش الحاسوب امر مختلف: حيث يستغرق وقتا أطول بكثير، وقد يتطلب

---

[82] Garrison notes these concerns: The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. Thus, the scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found. Id. (internal citations and quotations omitted).

[83] In United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), the Ninth Circuit considered a factual situation similar to a modern search through computer files: a search for a single document hidden somewhere in many boxes of documents. Rather than search through the boxes and seize only the one document, investigators carted off all the documents to search them off-site at a later time. The Ninth Circuit condemned the practice: It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment. As a general rule, in searches made pursuant to warrants only the specifically enumerated items may be seized. It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search. However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as the kind of investigatory dragnet that the fourth amendment was designed to prevent. We cannot sanction the procedure followed by the Government in this case. Id. at 595 (internal citations and quotations omitted). I am assuming in this discussion that the hardware is not also evidence or an instrumentality of crime. Where that assumption is incorrect, the hardware can be independently seized. See Davis, 111 F.3d at 1480 (computer used to store obscene images); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (computer used to store child pornography).

[84] . See generally Kremen v. United States, 353 U.S. 346 (1957) (per curiam) (holding that the Fourth Amendment does not permit seizure of a house and removal of its contents for subsequent examination).

[85] See supra notes 3-5 and accompanying text.

خبرة فنية كبيرة considerable technical expertise. والنهج الذي يعمل مع الأدلة المادية لا يعمل بشكل جيد مع الأدلة الرقمية.

ونتقدم سريعا إلى المرحلة التالية، حيث يقوم المحققون بإنشاء صورة تدفق البتات للحاسوب المضبوط. إن الحاجة إلى التنظيم القانوني واضحة. حيث تسمح عملية التصوير للحكومة بإعادة إنشاء نسختها المثالية من كل شيء على جهاز الحاسوب الخاص بالمشتبه به. بعد الحصول على نسختهم الخاصة، يتمتع المحققون بالقدرة التقنية على التنقيب عنها بحثا عن أدلة بلا حدود. يمكنهم التفتيش في النسخة لساعات أو أسابيع أو حتى سنوات. ومن اللافت للنظر أن قواعد التعديل الرابع التقليدية لا تفرض أي قيود على هذه العملية[86]. وبموجب القواعد التقليدية، فإن نسخ ملف الحاسوب لا يتم "ضبطه"، ويبدو أن تحليل نسخة الحكومة لا يشكل "تفتيشا"[87]. وتكمن المشكلة في التعريف التقليدي للضبط، الذي يظل مرتبطا بالمفهوم المادي لحرمان شخص آخر من ممتلكاته.

يحدث الضبط عندما يتسبب مسؤول حكومي في **"تدخل ذي مغزى في مصالح الحيازة للفرد في تلك الممتلكات"**[88]. ويعمل هذا الاختبار كدليل مفيد للحد من التدخل في الممتلكات المادية، لكنه يفشل عند تطبيقه على الأدلة الرقمية[89]. ولم يعد المحققون بحاجة إلى فرض تدخل ذي مغزى على مصلحة حيازية للحصول على أدلة رقمية. ولأن الشرطة يمكنها إنشاء نسخة كاملة من الأدلة دون حرمان المشتبه به من الممتلكات، فإن الوقائع الجديدة تفصل القاعدة عن وظيفتها التقليدية المتمثلة في الحد من تحقيقات الشرطة[90].

وفي المرحلة الأخيرة من التحقيق، يبحث المحققون في النسخة تفتيشا عن أدلة على الجريمة. وهذا يثير تهديدا للخصوصية نطلق عليه تسمية مشكلة إبرة في كومة قش needle-in-a-haystack problem. نظرا لأن أجهزة الحاسوب يمكنها تخزين كمية غير عادية من المعلومات، فإن أدلة الجريمة تشبه إبرة مخبأة في كومة قش إلكترونية ضخمة. إذا لم تكن هناك قواعد تنظم كيفية نظر المحققين من خلال كومة القش للعثور على

---

[86] See generally Kremen v. United States, 353 U.S. 346 (1957) (per curiam) (holding that the Fourth Amendment does not permit seizure of a house and removal of its contents for subsequent examination)

[87] See supra notes 3-5 and accompanying text.

[88] "meaningful interference with an individual's possessory interests in that property." See Arizona v. Hicks, 480 U.S. 321, 324 (1987) (holding that copying a serial number does not constitute a seizure); United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980) (holding that photocopying documents does not constitute a seizure because it is not a taking that involves dispossession). United States v. Jacobsen, 466 U.S. 109, 113 (1984)

[89] Courts have hinted in some cases that they might adopt a different definition of seizure in the context of electronic evidence, but those cases generally arise in the quite different context of interpreting Federal Rule of Criminal Procedure 41. Rule 41 authorizes warrants to seize "property," and several cases have raised the question whether this authority allows the police to use Rule 41 to authorize electronic monitoring or conduct so-called "sneak and peek" warrants. In that context, the courts have suggested that it is a seizure of property to view or copy information. See United States v. N.Y. Tel. Co., 434 U.S. 159, 169 (1977) (stating that Rule 41 "is broad enough to encompass a 'search' designed to ascertain the use which is being made of a telephone suspected of being employed as a means of facilitating a criminal venture and the 'seizure' of evidence which the 'search' of the telephone produces"); United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986) (holding that Rule 41 authorized a sneak and peek search in a case involving an illegal drug laboratory and that the property to be seized under the warrant "was information regarding the 'status of the suspected clandestine methamphetamine laboratory' ").

[90] See Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 Mich. Telecomm. & Tech. L. Rev. 39, 107 (2002) ("[T]he terms search and copy, as used with regard to electronic evidence, have different implications than the terms have in the physical world.").

الإبرة، فإن أي مبرر للتفتيش قد يبرر البحث الغازي justify an invasive من خلال ملفات الحاسوب التي تمثل قيمة المعلومات الخاصة لمدينة صغيرة.

تم تطوير قواعد التعديل الرابع الحالية لمنع هذا النوع من التفتيش العام في عمليات التفتيش عن الممتلكات المادية. حيث يجب أن يقتصر المكان المراد تفتيشه على موقع مادي محدد، مثل شقة أو مكتب، ويجب أن يكون التفتيش متسقا بشكل موضوعي مع البحث عن الأدلة المذكورة في المذكرة[91]. حيث تحاول القواعد ضمان أن تظل اجراءات التفتيش بناء على أوامر الاعتقال مصممة بشكل ضيق لمصلحة الحكومة.

ومع ذلك، فإن هذه القواعد لا تفعل الكثير لتنظيم عمليات التفتيش عن البيانات الإلكترونية. وتغير الأدلة الرقمية العلاقة بين حجم المساحة المراد التفتيش فيها وكمية المعلومات المخزنة داخلها. ففي العالم المادي، يحد شرط الخصوصية من نطاق التفتيش في مكان بناء على طلب منزل أو شقة. ويشكل الحد من المساحة المراد التفتيش فيها قيدا رئيسيا على نطاق التفتيش[92]. ولا ينطبق هذا القيد في حالة التفتيش في الحاسوب.

وفي أواخر عام 2004، كان القرص الصلب hard drive في جهاز حاسوب منزلي جديد نموذجي يخزن ما لا يقل عن أربعين غيغابايت من المعلومات[93]، أي ما يعادل تقريبا عشرين مليون صفحة من النصوص text أو حوالي نصف المعلومات المخزنة في الكتب الموجودة في طابق واحد من مكتبة أكاديمية نموذجية[94]. وبحلول الوقت الذي تقرأ فيه هذا المقال، ستكون السعة قد زادت بلا شك. تميل سعة تخزين محركات الأقراص الصلبة الجديدة إلى التضاعف كل عامين تقريبا[95]. بالنظر إلى كمية المعلومات التي يمكن تخزينها في قرص صلب صغير للحاسوب، ولم يعد شرط الخصوصية يخدم الوظيفة في قضايا الأدلة الإلكترونية بذات الشكل الذي يخدمها في قضايا الأدلة المادية. مهما كانت الوظيفة المتبقية التي تخدمها تتضاءل كل عام. واليوم،

---

[91] United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("Under Where... once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); United States v. Ewain, 88 F.3d 689, 692-93 (9th Cir. 1996) (noting that "once the police are lawfully searching in a place for one thing, they may seize another that is in plain view, if its incriminating nature is immediately apparent")

[92] As the Supreme Court suggested in United States v. Ross: Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab. 456 U.S. 798, 824 (1982).

[93] See, e.g., How to Buy A Desktop PC, at http://www.pcworld.com/howto/bguide/ 0, guid,14, page,3, 00.asp (last visited November 13, 2004) (on file with the Columbia Law Review).

[94] See, e.g., How Much Text Is in a Kilobyte or Megabyte, at http://www.wisegeek. com/how-much-text-is-in-a-kilobyte-or-megabyte.htm (last visited November 18, 2004) (on file with the Columbia Law Review) (explaining conversions of bytes to pages of text); Megabytes, Gigabytes, Terabytes ... What Are They? at http://www.pcsndreams.com/ Pages/Articles/Megabytes.htm (last visited November 18, 2004) (on file with the Columbia Law Review) (comparing measures of data stored digitally to the physical space required to store the same amount of data printed on paper).

[95] One can see this phenomenon in the rapidly outdated claims of how much storage space computer hard drives contain. See, e.g., Kevin J. Harrang, Licensing Issues in Creating and Publishing Multimedia Software Products, 418 PLI/Pat 289, 294 n.3 (1995) ("The typical hard disk of a personal computer..,. stores anywhere from about 40 to 400 megabytes of data."); Shira A. Scheindlin & Jeffrey Rabkin, Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?, 41 B.C. L. Rev. 327, 367 (2000) ("Hard drives that store 3000 to 4000 megabytes (or three to four 'gigabytes') are commonplace.").

قصر التفتيش على جهاز معين هو شيء مثل قصر التفتيش على كتلة المدينة. بعد عشر سنوات من الآن، سيكون الأمر أشبه بقصر التفتيش على المدينة بأكملها.

وقد انذرت هذه المشكلة إلى حد ما بحالات مادية تنطوي على العديد من صناديق الوثائق الورقية. لكن عمليات التفتيش عن المستندات الورقية لم تتسبب في نفس ترتيب حرقة القلب heartburn الذي ستثيره عمليات التفتيش عن ملفات الحاسوب، ولم تطلق قواعد جديدة لمعالجة مشكلة إبرة كومة القش. حيث تبرز قضية Andresen v. Maryland تلك الديناميكية[96].

وفي قضية أندرسن Andresen هذه، قامت الشرطة بالتفتيش في الملفات الورقية في مكتب محام عن أدلة على الاحتيال المتعلق بصفقة عقارية. واعترض المتهم قائلا إن الأمر لم يكن محددا بما فيه الكفاية، ولكن المحكمة العليا وافقت بسهولة على الأمر. وأوضحت المحكمة أنه من الكافي معالجة مشكلة الإبرة في كومة قش مع وضع جانب عام فقط في حاشية: "نحن ندرك أن هناك مخاطر جسيمة grave dangers" متأصلة في عمليات التفتيش عن الوثائق[97]. و"في عمليات التفتيش في الأوراق، من المؤكد أنه سيتم فحص بعض المستندات غير الضارة، على الأقل بشكل سريع، من أجل تحديد ما إذا كانت كذلك، وفي الواقع، من بين تلك الأوراق المصرح بمصادرتها"[98]. قدمت المحكمة تحذيراً warning ولكن لم تقدم قاعدة قانونية لمعالجة هذه المشكلة، وذكرت فقط أن "الموظفين المسؤولين ... يجب أن يحرصوا على التأكد" من أن عمليات التفتيش هذه "تتم بطريقة تقلل من التدخلات غير المبررة في الخصوصية"[99].

ولا يمكن استعادة الوظيفة المفقودة لشرط الخصوصية في التفتيش عن الأدلة الرقمية بمجرد اشتراط مزيد من التحديد. حيث انه لا تمنحنا التكنولوجيا الحالية أية طريقة لمعرفة مكان وجود ملف أو معلومة معينة داخل الحاسوب مسبقا. ففي العالم المادي، يتم استخدام مناطق مكانية مختلفة لأغراض مختلفة. يسمح هذا للشرطة بإجراء تخمينات مستنيرة حول المكان الذي قد يتم العثور فيه أو عدم العثور على الأدلة، مما يسمح لهم بتوليد طرق للحد من التفتيش. ضع في اعتبارك المذكرة التي تم الحصول عليها لتفتيش منزل فريد فيلوني في التحقيق في سرقة بنك العالم المادي. حيث يمكن أن تقتصر مذكرة التوقيف على منزل فريد لأنه من غير المرجح أن يخزن الأدلة في الشارع أو في حديقة عامة. ومع ذلك، واما في سياق الحاسوب، يتم تحديد قرار مكان وضع معلومات معينة داخل جهاز التخزين في المقام الأول من خلال برنامج معين مثبت والأسئلة الطارئة حول ما يحدث أيضا ليتم تخزينه على نفس محرك التخزين[100]. وبالنسبة للجزء الأكبر، من المستحيل معرفة ذلك قبل الاستيلاء على العنصر وتحليله في المعمل الشرعي الرسمي government's lab.

حتى في الإعداد الخاضع للرقابة للمعمل الشرعي، تفشل قواعد التعديل الرابع الحالية في توليد أدلة مفيدة لإجراء التحقيق. ضع في اعتبارك قيدين قانونيين محتملين على نطاق بحث محلل المعمل الشرعي: أولا، حدود مناطق القرص الصلب التي يمكن للمحلل البحث عن الأدلة المذكورة فيها، وثانيا، القيود المفروضة على قدرة المحلل على التفتيش عن أدلة عن جرائم أخرى. قاعدة التعديل الرابع العامة هي أن المحققين الذين ينفذون مذكرة يمكن أن يبحثوا في أي مكان في المكان المراد تفتيشه حيث يمكن تصور وجود الأدلة الموضحة

[96] Andresen v. Maryland 427 U.S. 463 (1976).
[97] Id. at 482 n.ll.
[98] "In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Id.
[99] Id.
[100] See generally Nelson et al., supra note 20, at 73-158 (reviewing various types of file systems, structures, and storage).

في المذكرة[101]. وفي التحقيقات التقليدية للحصول على أدلة مادية تعني هذه القاعدة أنه لا يمكن للضبط القضائي التفتيش في أماكن أصغر من الأدلة التي يرغبون في ممارسة الضبط عليها. فإذا كان لدى الشرطة أمر لاستعادة مسدس، فإن الأمر لا يبرر فتح خطاب شخصي. لكن الأدلة الإلكترونية يمكن أن تكون موجودة في أي مكان. يمكن تسمية الملفات بشكل خاطئ أو إخفاؤها أو تخزينها بطريقة أخرى بطريقة لا يمكن للمحقق أبدا استبعاد جزء معين من القرص الصلب مسبقا[102]. ونتيجة لذلك، يمكن للضباط التفتيش في كومة القش الرقمية بأكملها للعثور على الإبرة[103]". حيث تفرض القاعدة التقليدية حدا كبيرا لعمليات التفتيش المادية، ولكن ليس للتفتيش عن الأدلة الإلكترونية electronic evidence.

يحدث الشيء نفسه مع القواعد التي تفرض نطاق الأمر scope of the warrant. عندما يتم مصادرة أدلة تتجاوز مذكرة التوقيف بموجب استثناء الرؤية الواضحة plain view exception، يتحرك المتهمون بشكل روتيني للمطالبة برفض تلك الأدلة على أساس أنها اكتشفت في تفتيش تجاوز نطاق الأمر exceeded the warrant's scope. ويدعو القانون الحالي القضاة إلى تجاهل نية الضابط الذاتية للتفتيش عن أشياء تتجاوز المذكرة[104]". حيث يسأل المبدأ بدلا من ذلك عما إذا كان التفتيش الذي أجراه مأمور الضبط بالفعل متسقا بشكل موضوعي مع نوع التفتيش الذي يمكن إجراؤه بشكل معقول عن الأدلة التي تصفها المذكرة[105]. وإذا كان الأمر كذلك، فيمكن قبول الأدلة غير ذات الصلة بموجب استثناء الرؤية الواضحة. إذا لم يكن الأمر كذلك، يتم رفض الأدلة evidence is suppressed.

تبدو هذه القاعدة معقولة في سياق التفتيش عن أدلة مادية context of a search for physical evidence. وقد يكون من الصعب معرفة النية الذاتية لمأمور الضبط، ولكن من الممكن عموما قياس ما إذا كانت خطوات مأمور الضبط متسقة مع عمليات التفتيش عن أنواع معينة من الأدلة. فقد يبدو التفتيش عن تلفزيون مسروق مختلفا عن التفتيش عن فواتير ورقية مسروقة. غير أن القاعدة لا تفرض حدا حقيقيا على إجراءات التفتيش عن الأدلة الإلكترونية. نظرا لأنه يمكن وضع الأدلة الإلكترونية في أي مكان على القرص

---

[101] United States v. Ross, 456 U.S. 798, 824 (1982)

[102] See United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (noting that agents executing a search for computer files are "not required to accept as accurate any file name or suffix and [to] limit [their] search accordingly" because criminals may "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories"); United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000, at *4 (W.D. Mich. Aug. 30, 1991) (stating that "the police were not obligated to give deference to the descriptive labels placed on the discs by [the defendant]. Otherwise, records of illicit activity could be shielded from seizure by simply placing an innocuous label on the computer disk containing them")

[103] See United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) (stating that when searching computer data for information whose nature cannot be known in advance, "law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location").

[104] See United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder Whren, .. . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996) ("Using a subjective criterion would be inconsistent with Horton, and would make suppression depend too much on how the police tell their story, rather than on what they did.").

[105] See United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder Whren, .. . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search is irrelevant."); United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996) ("Using a subjective criterion would be inconsistent with Horton, and would make suppression depend too much on how the police tell their story, rather than on what they did.").

الصلب، فمن الصعب، إن لم يكن من المستحيل، القول إن تفتيشا معينا كان غير مبرر بشكل موضوعي. فلا تمنع قواعد العالم المادي التفتيش العام في الأدلة الإلكترونية[106].

وأخيرا، لا يفرض القانون الحالي حدودا زمنية على التفتيش في الحواسيب ولا يولي اهتماما كبيرا لزمان أو ما إذا كان يجب إعادة الحواسيب المضبوطة. ولا يتطلب التعديل الرابع ولا القواعد الفيدرالية للإجراءات الجنائية من الضبط القضائي بدء عملية فحص المعمل الشرعي forensic examination process بطريقة سريعة [107]. اذ بمجرد ضبط الحاسوب، يمكن للشرطة عادة الاحتفاظ به إلى أجل غير مسمى indefinitely [108]. فلا يوفر القانون الفيدرالي سوى آلية محدودة للغاية لإعادة الممتلكات التي تم ضبطها بموجب أمر قضائي[109]؛ حيث يجب على المشتبه به suspect تقديم طلب لاستعادة ممتلكاته المضبوطة motion seeking a return of property وإثبات إما أن الضبط كان غير قانوني أو أن الحكومة لم تعد بحاجة إلى الاحتفاظ بالأدلة retain the evidence.

"إذا لم يقدم أي التماس، فلا يلزم إعادة الممتلكات. حتى إذا تم تقديم طلب وتمت الموافقة عليه، فإن الأمر باستعادة الحاسوب لا يتطلب من الشرطة إعادة أو إتلاف نسخة bitstream التي أنشأتها.[110] ونظرا لأن القاعدة الحالية تركز على مصلحة ملكية المشتبه به بدلا من مصلحة الخصوصية، ويمكن للشرطة الاحتفاظ بالنسخة ومواصلة البحث فيها دون حد واضح. فقد تكون هذه القواعد منطقية بالنسبة للممتلكات المادية ولكنها

[106] Cf. Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994) (describing the "intermingled documents problem" of Fourth Amendmentjurisprudence and its relevance for computer searches). The problem is particularly significant because other digital files may support a more severe and more easily proven criminal charge. When searching through Fred's computer files, for example, agents would have a strong incentive to check to see if it happens to contain any images of child pornography. The possession of child pornography carries very high felony penalties. See, e.g., United States v. DeBeir, 186 F.3d 561, 567 (4th Cir. 1999) (calculating a sentence under U.S. Sentencing Guidelines). Smart investigators would know that if they find child pornography images on the hard drive, they could drop the bank theft charges against Fred and charge him with possessing child pornography instead. See, e.g., United States v. Carey, 172 F.3d 1268, 1273-74 (10th Cir. 1999) (discussing search through computer for drug-related evidence that led to child pornography charges); United States v. Turner, 169 F.3d 84, 86 (1st Cir. 1999) (explaining how a search through computer for evidence of assault led to child pornography charges); see also Gray, 78 F. Supp. 2d at 526-27 (explaining how search through computer for evidence of computer hacking led to child pornography charges).

[107] United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (holding that Rule 41 does not "provide[ ] for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant").

[108] See DOJ Manual, supra note 12, at 77 ("The government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner without legal restrictions ....").

[109] Fed R. Crim. P. 41(g) ("A person aggrieved by... the deprivation of property may move for the property's return.").

[110] See Ramsden v. United States, 2 F.3d 322, 326 (9th Cir. 1993) (stating that "[t]he United States' retention of the property generally is reasonable if it has a need for the property in an investigation or prosecution. However, 'if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable" (quoting Fed. R. Crim. P. 41(e) advisory committee's notes (proposed amend. 1989))).

تظهر نقصا مفاجئا في الاهتمام بالمصالح المشروعة التي يتمتع بها مستخدمو أجهزة الحاسوب والملفات الخاصة بهم[111].

III. نحو قواعد جديدة للإجراءات الجنائية

III. TOWARD NEW RULES OF CRIMINAL PROCEDURE

لقد كلفت تقاليدنا الدستورية القضاة بتنفيذ شرعة الحقوق من خلال قواعد محددة. تتطور هذه القواعد بطريقة مجزأة بمرور الزمن. ففي حالة التعديل الرابع، ولد التنفيذ القضائي بنية عقائدية معقدة تملأ عدة مجلدات في الأطروحات الرائدة"[112]. ويحاول هذا المبدأ تفعيل حظر التعديل الرابع ضد "عمليات التفتيش والضبط والمصادرة غير المعقولة unreasonable searches and seizures" وتاريخ القلق من الأوامر العامة من خلال قواعد محددة تحكم ما يمكن وما لا يمكن للسلطات القيام به في حالات محددة.

حيث تكشف الأدلة الرقمية عن طوارئ القواعد الحالية. ويكشف كيف أن القواعد التي تم وضعها لتنفيذ القيود الدستورية على جمع الأدلة تستند إلى ديناميات الجرائم المادية والأشكال التقليدية للأدلة المادية وشهادات شهود العيان. فعندما يتم تطبيق قواعد التنفيذ هذه على حقائق جمع الأدلة الرقمية، فإنها لم تعد وفية للغرض الذي وضعت لتحقيقه. اذ تتولى الأدلة الرقمية تغيير الافتراضات الأساسية للعالم المادي التي أدت إلى القواعد السابقة، مشيرة إلى النتائج التي لم تعد تعكس الأهداف والأغراض الأساسية للتعديل الرابع.

وبالمعنى الضيق، هذا ليس شيئا جديدا. ذلك إن تطور التعديل الرابع لكي يستجيب للتكنولوجيا هو قصة قديمة، ربما يعود تاريخها إلى أول حالة استثناء للسيارات في عام1925 [113] وفي الآونة الأخيرة، تم تصميم اختبار **"التوقع المعقول للخصوصية reasonable expectation of privacy"** من قضية كاتز ضد الولايات المتحدة Katz v. United States لتحديث التعديل الرابع للمساعدة في تنظيم المراقبة الهاتفية، وعلى نطاق أوسع لتحقيق نوع من الحياد التكنولوجي في قانون التفتيش والضبط search and seizure law"[114] .

وبالمثل Similarly، شهدت المحاكم قضايا تتعلق بوثائق ورقية paper documents لسنوات"[115]. كل هذا صحيح، ولكنه لا يروي سوى جزء من القصة. في حين شددت قضية كاتس Katz على الحاجة إلى التغيير، إلا أن تأثيرها على القانون كان ضيقا بشكل مدهش. فقد ركزت قضية كاتز Katz فقط على السؤال الأولي حول ما يعتبر "تفتيشا search"، وكما أوضحت في مكان آخر elsewhere، كان له تأثير ضئيل

---

[111] See id. at 327 (requiring government to return original set of documents but noting that it can keep a set of copies).
[112] See, e.g., Wayne R. La Fave, Search and Seizure: A Treatise on the Fourth Amendment (3d ed. 1996).
[113] nt (3d ed. 1996). 114. See Carroll v. United States, 267 U.S. 132, 149 (1925) (holding that an automobile can be searched without a warrant if probable cause exists to believe contraband was stored within it). The rule announced in Carroll was based, at least in part, on the technological reality of automobiles. A warrant requirement would not be practicable, the Court noted, "because the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought." Id. at 153. The rule also appeared to factor in the social realities of automobile use in the Prohibition era. Probable cause was required, the Court suggested, because "[i]t would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search." Id. at 153-54.
[114] Katz v. United States 389 U.S. 347, 353 (1967).
[115] See supra text accompanying notes 97-100.

بشكل مدهش على قانون التعديل الرابع ككل[116]. وعلى نفس المنوال، لم تستجب المحاكم لعمليات التفتيش عن المستندات الورقية من خلال إنشاء قواعد جديدة لتنظيم عمليات التفتيش الورقية[117]. وفي حين أن القضايا التي تنطوي على الهواتف والمستندات الورقية أدخلت التحول المفاهيمي من الأدلة المادية إلى أشكال البيانات الخام أكثر rawer forms of data، وهي ليست شائعة ولا مختلفة كثيرا neither so common nor so different عن القضايا التقليدية بحيث أحدثت تحولات كبيرة triggered major shifts في قانون الإجراءات الجنائية law of criminal procedure.

ويثير الاعتماد المتزايد على أجهزة الحاسوب في كل جانب من جوانب الحياة الأمريكية تقريبا اعتبارات مختلفة تماما. لاحظ جاك بالكين Jack Balkin أنه عندما نفكر في تأثير التقنيات الجديدة على القانون، فإن القضية ليست انها جديدة بل بارزة[118]. **" فما هي عناصر العالم الاجتماعي التي تجعل التكنولوجيا الجديدة بارزة بشكل خاص والتي لم يلاحظها أحد نسبيا من قبل؟ . . . وما هي العواقب. . . لجعل هذا الجانب أكثر أهمية أو أكثر انتشارا أو أكثر مركزية مما كان عليه من قبل؟"**[119] فلم نعد نتعامل مع الميكروفونات المسجلة على أكشاك الهاتف أو أكوام الأوراق الموجودة في خزائن الملفات. اليوم يتم إجراء جزء متزايد من حياتنا عبر وسيط أجهزة الحاسوب. بحيث أصبح جمع الأدلة الرقمية وتحليلها جزءا روتينيا وأساسيا بشكل متزايد من مجموعة واسعة من التحقيقات الجنائية. حيث يتحد اعتمادنا المجتمعي على أجهزة الحاسوب مع الاختلافات بين الأدلة المادية والأدلة الرقمية لتوليد حاجة ملحة لإعادة التفكير في القواعد الإجرائية التي تحكم جمع الأدلة الرقمية.

جادل لورانس ليسيغ Lawrence Lessig بأن المحاكم يجب أن تشارك في "الترجمة translation" عندما تطبق الدستور على الإنترنت[120]. والترجمة هي محاولة لتحديث قواعد القانون استجابة للتقنيات المتغيرة والممارسة الاجتماعية[121]. وهو ما يبرر تغيير القواعد العقائدية لضمان بقاء الدور basic role والوظيفة function الأساسيين للأوامر الدستورية ثابتين عبر الزمن. فعلى سبيل المثال، يجادل ليسيغ Lessig بأن التعديل الرابع يجب أن يفهم على أنه أمر عام لحماية الخصوصية privacy[122]. وعند تطبيق التعديل الرابع على الإنترنت، يقترح أن يتبنى القضاة قواعد تحمي الخصوصية بالنظر إلى حقائق كيفية عمل الإنترنت[123]. يقدم نهج ليسيغ Lessig احتمالات مثيرة للاهتمام interesting possibilities، لكنه لا يولد سوى إجابة جزئية. في حين تسمح الترجمة بالتطور العقائدي استجابة للتقنيات والممارسات الاجتماعية المتغيرة، إلا أنها تظل حبيسة الترتيبات المؤسسية الموجودة مسبقا preexisting. وهو يتطلب من المحاكم أن تضطلع بالدور الذي اضطلعت به تقليديا وأن تأخذ زمام المبادرة في إعادة تشكيل القواعد في ضوء التغير التكنولوجي in light of technological change.

---

[116] See Kerr, New Technologies, supra note 32, at 807.
[117] See supra notes 97-100 and accompanying text.
[118] Jack M. Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79 N.Y.U. L. Rev. 1, 2 (2004).
[119] "What elements of the social world does a new technology make particularly salient that went relatively unnoticed before? . . . And what are the consequences . . . of making this aspect more important, more pervasive, or more central than it was before?" Id. at 2-3.
[120] See generally Lawrence Lessig, Code and Other Laws of Cyberspace (1999) [hereinafter Lessig, Code]; Lawrence Lessig, Fidelity as Translation, 71 Tex. L. Rev. 1165 (1993).
[121] See Lessig, Code, supra note 121, at 114.
[122] See id. at 115.
[123] See id. at 115-16.

والنهج الأفضل هو فتح احتمالات open the possibilities إجراء جنائي جديد أمام ترتيبات مؤسسية جديدة. ويلزم أن تحتفظ المحاكم بدور مهم: عندما تتناسب التغييرات المطلوبة بشكل جيد مع النطاق والأغراض التقليدية لقواعد التعديل الرابع، بحيث يمكن للمحاكم إعادة تصميم القواعد الحالية في ضوء الحقائق الجديدة. لكن هذا النهج التطوري ليس سوى جزء من استجابة أوسع يمكن أن تقدمها المؤسسات القانونية. اذ ان بعض التحديات الجديدة التي أثارتها الأدلة الرقمية ترسم خريطة واضحة لمبادئ التعديل الرابع التقليدية؛ والبعض الآخر لا تستطيع ذلك. وعندما لا تفعل ذلك، هنا، يمكن للهيئات التشريعية والوكالات التنفيذية تقديم حلول جديدة ومبتكرة لتنظيم جمع الأدلة الرقمية.

وفي حين أن السلطة القضائية مقيدة بالتأمل stare decisis، فانه يمكن للسلطتين التشريعية والتنفيذية legislative and executive branches تجربة مجموعة واسعة من المقاربات[124]. ويمكنهما تحديد وسن قواعد جديدة استجابة لديناميات التكنولوجيات الجديدة. وبالإضافة إلى ذلك، يمكن للهيئات التشريعية والوكالات التنفيذية تنظيم الحلول الشاملة دون انتظار ظهور القضايا والخلافات[125].

وتشير المرونة الأكبر في وضع القواعد في السلطتين التشريعية والتنفيذية إلى أنه لا ينبغي لنا أن ننظر فقط إلى المحاكم. وكما أوضحت مؤخرا في مكان آخر، تشير الصعوبات المؤسسية النسبية التي يواجهها القضاء في تنظيم التقنيات المتطورة إلى أن الفروع الأخرى يجب أن تلعب دورا مهما[126]. بحيث يجب أن نعيد التفكير في القانون وأغراضه من المبادئ الأولى، والنظر إلى ما وراء التقاليد الدستورية التي عملت بفعالية في القضايا التقليدية ولكنها قد لا تثبت أنها كافية تماما عند تطبيقها على الأدلة الرقمية.

يقدم هذا الجزء بعض الأفكار المبدئية حول الحلول التي قد يعتمدها النظام القانوني استجابة للحقائق الجديدة للآليات الأساسية الثلاث لجمع الأدلة الرقمية. هدفها الأساسي هو البدء في التفكير في حلول جديدة، بدلا من وضع مقترحات مفصلة. هدفها الثانوي هو إظهار أن مثل هذه التغييرات ربما تكون قد بدأت تحدث بالفعل.

فقد بدأت تظهر مجموعة جديدة من القواعد المطبقة في التحقيقات المتعلقة بجرائم الحاسوب. حيث قام كل من الكونغرس والمحاكم بالفعل بتغيير العديد من قواعد الإجراءات الجنائية استجابة للحقائق الجديدة للتحقيقات في جرائم الحاسوب. وكان الكونجرس هو الفاعل الرئيسي على مرحلتين: فقد سن قواعد لتنظيم كل من عملية الاستدعاء subpoena process والمراقبة المستقبلية prospective surveillance بطرق تبدأ في تلبية الاحتياجات المستقبلية. وكانت المحاكم نشطة في المرحلة الثالثة، التي تنطوي على اجراء المعمل الشرعي الحاسوبي computer forensics process. والخطوات المتخذة حتى الآن متواضعة. فبعض التدابير القضائية هي مقترحات المحاكم الدنيا التي يمكن عكسها/ رفضها في الاستئناف أو إضعافها من خلال القرارات المستقبلية، وبعضها يتقاطع مع جوهر القضايا الأخرى حول نفس المسألة. ويحتاج العديد من التدابير التشريعية legislative measures إلى قدر كبير من العمل. ومع ذلك، من المرجح أن تمثل هذه التطورات القانونية والدستورية مجتمعة بداية فرع جديد من الإجراءات الجنائية مصمم خصيصا لتنظيم الأدلة الرقمية- وهو فرع أكثر استجابة وتنوعا مؤسسيا من القانون الموجود اليوم.

[124] See Kerr, New Technologies, supra note 32, at 166-69 (noting different operative constraints of judicial and legislative branches).
[125] See id. at 163-66.
[126] See generally id.

A. جمع الأدلة المخزنة من أطراف ثالثة

A. Collection of Stored Evidence from Third Parties

ضع في اعتبارك الخطوة الأولى لمعظم التحقيقات في جرائم الحاسوب، وهي جمع الأدلة المخزنة من مزودي الخدمات وهو الطرف الثالث. اذ تؤدي الزيادة في كمية وأهمية المعلومات المخزنة عند أطراف ثالثة في بيئة الشبكة إلى الحاجة إلى قيود جديدة على سلطة الاستدعاء subpoena power. ويأتي الحد الأكثر وضوحا في شكل عتبة قانونية أعلى a higher legal threshold للإجبار على الإفصاح compel disclosure؛ اذ يجب أن يشترط القانون عرضا واقعيا أكثر إرهاقا للحصول على معلومات خاصة عن المشتبه بهم، مثل بريدهم الإلكتروني الشخصي. ويمكن النظر في حدود أخرى أيضا.

وربما يجب أن يحد القانون من عدد الحسابات المستهدفة التي يمكن إجبارها بالكشف في أي وقت، على الأقل في غياب مبرر خاص absent special justification. وربما ينبغي اشتراط إشعار مسبق prior notice في بعض الحالات، أو إبلاغ المستهدفين بالتحقيقات في غضون فترة زمنية بعد حدوث الكشف. وقد تكون قيود الاستخدام طريقة جيدة للحد من المخاطر الناشئة عن الإفصاحات الواسعة. وعلى سبيل المثال، قد يحظر القانون على السلطات استخدام المعلومات القسرية من مزود الخدمة لغرض لا علاقة له بالكشف الأولي. بدلا من ذلك، قد يطلب من السلطات حذف المعلومات بعد فترة من الوقت، ربما ثلاثين يوما. حيث يجب أن تستجيب القواعد الجديدة لتهديدات الخصوصية الجديدة التي يثيرها امتلاك طرف ثالث للمعلومات الخاصة التي أصبحت شائعة بواسطة شبكات الحاسوب والإنترنت.

وعلى الرغم من أن المحاكم لم تتخذ أية خطوات نحو مثل هذا النظام، إلا أن الكونجرس فعل ذلك. أظهر الكونجرس بصيرة ملحوظة من خلال سن قواعد لتضييق نطاق سلطة الاستدعاء subpoena power منذ عام 1986، عندما أقر الكونجرس قانون خصوصية الاتصالات الإلكترونية[127]. في شكله الحالي، حيث تظهر القواعد التي تحد من سلطة الاستدعاء في القسم 18 U.S.C.2703 حيث يفرض القسم 2703 Section قيودا قانونية على كيفية حصول الحكومة على المعلومات من مزودي خدمات الإنترنت.

وعلى الرغم من أن التشريع المذكور لا يزال غير مفهوم بشكل جيد، إلا أنه يتطلب من السلطات law enforcement تلبية عرض أعلى من أمر استدعاء subpoena للحصول على معلومات خاصة تتعلق بالعملاء والمشتركين في مزودي خدمات الإنترنت[128]. وعندما يسعى المحققون للحصول على معلومات خاصة مثل رسائل البريد الإلكتروني التي لم يتم تسليمها، يجب عليهم أولا الحصول على أذن تفتيش بناء على سبب محتمل.[129]" حيث يفرض القانون شرطا أقل من أمر محكمة "حقائق محددة وواضحة specific

---

[127] Pub. L. No. 99-508, 100 Stat. 1848 (1986). Section 2703 imposes statutory restrictions on how the government can obtain information from ISPs.

[128] I explain section 2703 in considerable depth in Orin S. Kerr, A User's Guide to the Stored Communications Act-and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1218-20 (2004) [hereinafter Kerr, User's Guide].

[129] 18 U.S.C. ? 2703(a) (2000). This section states: A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. Id.

and articulable facts" للحصول على بعض المعلومات الأخرى،[130] ويفرض أيضا شرط الإشعار المسبق للمستخدم في سياقات معينة. ولقد شرحت هذا النظام الأساسي بالتفصيل في مكان آخر، ولن أفعل ذلك هنا."[131] فالمفتاح هو أن الكونجرس قد تدخل وبدأ في معالجة كيف يجب أن تغير بنية التحقيقات الجديدة القواعد القديمة. النظام القانوني ليس مثاليا، لكنه يبدأ في إعادة القانون إلى شيء أقرب إلى التوازن الذي يصل إليه في التحقيقات التقليدية.

B. المراقبة المستقبلية

B. Prospective Surveillance

وتتطلب آليات المراقبة المرتقبة The mechanisms of prospective surveillance أيضا نظاما قانونيا جديدا. وتتمثل الحاجة الأساسية في أن تركز العتبات القانونية ذات الصلة relevant legal thresholds، قدر الإمكان استنادا إلى التكنولوجيا الموجودة، على نوع المعلومات التي يتعين جمعها بدلا من التركيز على ما إذا كان المكان المراد الدخول اليه عاما أم خاصا. يجب أن تحاول القواعد ربط العرض المطلوب لإجراء المراقبة بدرجة تهديد الخصوصية الذي يثيره هذا النوع من المراقبة.

عند تكوين عامل تصفية لجمع معلومات من نوع يميل إلى أن يكون خاصا، يجب أن تكون هناك حاجة إلى حد عالي. وفي المقابل، ينبغي السماح بالمراقبة المرتقبة تحت عتبة أدنى عندما يتم جمع معلومات أقل خصوصية. سوف يتطلب هذا النهج من القانون تصنيف اتصالات الإنترنت بناء على درجة مصالح الخصوصية المعرضة للخطر. وعلى سبيل المثال، قد يكون من المفيد أن يكون لديك فئة واحدة للمواد الخاصة جدا مثل رسائل البريد الإلكتروني، وفئة وسيطة للمعلومات المتعلقة بعادات تصفح الويب، وعتبة ثالثة لمعلومات الخصوصية المنخفضة مثل رؤوس بروتوكول الانترنت IP headers أو اتصالات الهكرة hacker communications.

قد يكون المزيد من الخيارات الإبداعية يستحق الاستكشاف أيضا. تثير مراقبة الإنترنت المرتقبة Prospective internet surveillance مشكلة إبرة في كومة قش a needle-in-the-haystack problem: يجب ضبط الفلتر/ المرشح filter بحيث يلتقط الإبرة needle ولكن ليس القش hay. توجد مجموعة من الآليات mechanisms للمساعدة في تركيز العملية. ويتمثل أحد الخيارات في اعتماد استراتيجيات التقليل إلى أدنى حد من قانون التنصت Wiretap Act على المكالمات الهاتفية وتطبيقها على نطاق أوسع على جميع أشكال المراقبة المحتملة[132].

على سبيل المثال، قد يتطلب القانون من أطراف ثالثة محايدة مراجعة الأدلة التي تم جمعها من خلال المراقبة المستقبلية قبل نقلها إلى السلطات. وبدلا من ذلك، يمكن للقانون تنظيم أنواع الأدوات المستخدمة لضمان استخدام أكثر الأدوات فعالية، أو قد يتطلب التسجيل أو حفظ السجلات بواسطة تلك الأدوات لإنشاء سجل

[130] Id. ? 2703(d). The section states that: A court order for disclosure . . . may be issued by any court that is a court of competent jurisdiction . . . and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. Id.
[131] Id. Sec. 2703(b).
[132] See 18 U.S.C. ? 2518. See generally United States v. Scott, 504 F.2d 194, 198-99 (1974) (discussing section 2518's minimization requirements in context of telephone wiretap).

لكيفية استخدامها. أثيرت بعض هذه الأفكار في النقاش حول برنامج المراقبة المرتقبة لمكتب التحقيقات الفيدرالي المعروف أحيانا باسم كارنيفور Carnivore [133] حيث يجب طرح ذات الأسئلة على نطاق أوسع حول أي منهج محتمل للمراقبة any method of prospective surveillance.

وقد اتخذ الكونغرس بالفعل بضع خطوات مبدئية tentative steps في مثل هذا الاتجاه، وإن لم يكن ذلك من دون إثارة جدل كبير. وتم تعديل القانون الوطني الأمريكي لعام 2001 (قانون باتريوت) قانون خصوصية الاتصالات الإلكترونية من خلال تقسيم المراقبة المرتقبة إلى فئتين[134]. الفئة الأولى هي المراقبة المستقبلية لـ.. "محتويات contents" الاتصالات[135]، والثانية هي المراقبة المستقبلية لـ "معلومات الاتصال dialling أو التوجيه routing أو العنونة addressing أو الإشارة "signalling (DRAS) [136].

الفئة الأولى هي فئة الاتصالات الأكثر خصوصية more private category of communication: على الرغم من أن نطاقها ليس واضحا تماما[137]، إلا أنها تشمل محتويات رسائل البريد الإلكتروني وربما نص أوامر الإنترنت internet commands[138] ومصطلحات التفتيش search terms[139]. والأخيرة هي فئة الاتصالات الأقل خصوصية، بما في ذلك رؤوس حزم الإنترنت internet packet headers، وعناوين البريد الإلكتروني e-mail addresses، والبيانات data الأخرى المستخدمة لتوجيه اتصالات الإنترنت routing internet communications (و، من المفترض أن أي شيء آخر ليس محتويات)[140]. وبموجب قانون الطوارئ/ باتريوت the Patriot Act، يتم تنظيم المراقبة المستقبلية التي تجمع DRAS فقط من خلال تشريع التسجيل Pen Register Statute منخفض الحماية[141].

---

[133] 135. See, e.g., IIT Research Inst., Independent Technical Review of the Carnivore System Draft Report (2000), available at http://www.usdoj.gov/jmd/publications/ carnivore_draft_l.pdf (on file with the Columbia Law Review); IIT Research Inst., Independent Technical Review of the Carnivore System Final Report (2000), available at http://www.usdoj.gov:80/jmd/publications/carnivfinal.pdf (on file with the Columbia Law Review) (emphasizing need for postcollection auditing of uses of Carnivore).

[134] See generally Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, ? 216, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (amending generally 18 U.S.C. ?? 3121-3127).

[135] See generally Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, ? 216, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (amending generally 18 U.S.C. ?? 3121-3127).

[136] 3127). 137. See 18 U.S.C. ? 2510(8) (defining "contents" for wire or electronic communication as that which "includes any information concerning the substance, purport, or meaning of that communication"). This provision was enacted in 1968 and amended in 1986. See Kerr, Internet Surveillance, supra note 10, at 647 n.194.

[137] See United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000)

[138] See United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). 141. In re Pharmatrak Inc., 329 F.3d 9, 18-19 (1st Cir. 2003).

[139] In re Pharmatrak Inc., 329 F.3d 9, 18-19 (1st Cir. 2003).

[140] See Kerr, Internet Surveillance, supra note 10, at 644-48 (describing status of these data in statutory surveillance regimes).

[141] 18 U.S.C. ?? 3121-3127 (Supp. 2002); see DOJ Manual, supra note 12, at 111-12. 144. Section 3121(b) lists the exceptions, which include monitoring conducted in the following circumstances:
(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

يحتاج مأمور الضبط القضائي إلى الحصول على أمر محكمة ذي صلة فقط لإجراء المراقبة، أو ملاءمة المراقبة ضمن واحد من عدة استثناءات قانونية واسعة[142]. وفي المقابل، يتم تنظيم المراقبة المستقبلية التي تجمع المحتويات بموجب قانون التنصت على المكالمات السلكية الهاتفية Wiretap Act عالي الحماية[143]. ويجب على مأمور الضبط القضائي الحصول على أذن تفتيش search warrant "فائق super" (يعادل الاذن من القاضي الجزئي)[144] قبل إجراء المراقبة، وإلا فإن سلوكها يندرج ضمن واحد من عدة استثناءات قانونية ضيقة نسبيا narrow statutory exceptions."[145] ويضيف قانون الطوارئ أيضا شرط البلاغ reporting requirement الذي يتطلب في بعض السياقات من السلطات تقديم تقارير عن استخدام المراقبة المرتقبة إلى المحكمة التي أذنت بالمراقبة[146].

يتضمن قانون الطوارئ ابتكارا آخر: فهو يضيف استثناء إلى قانون التنصت على المكالمات السلكية/ الهاتفية Wiretap Act لإعفاء اتصالات الهكرة hackers المرسلة عبر حاسوب الضحية[147]. وبموجب هذا الحكم، يمكن لضحية الهكترة أن يسمح للسلطات بإجراء مراقبة مستقبلية لاتصالات الهكر إذا كانت هناك "أسباب معقولة للاعتقاد بأن اتصالات المتعدي ستكون ذات صلة بالتحقيق"[148].

تقدم سرقة بنك فريد عبر الإنترنت مثالا. إذا استخدم ممثلو المكتبة العامة كضحية وسيطة لمراقبة تدخلات فريد المستقبلية. فإذا اخترق فريد حاسوب المكتبة مرة أخرى، فستتمكن الحكومة من مراقبة اتصالات فريد دون الحصول أولا على أمر قضائي. الفكرة وراء ما يسمى استثناء المتعدي trespasser exception وهي تكييف قواعد المراقبة مع مصلحة الخصوصية في الاتصالات عبر الإنترنت. ولأن مخترق الحاسوب ليس

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3) where the consent of the user of that service has been obtained. 18 U.S.C. ? 3121(b) (2000)

[142] Section 3121(b) lists the exceptions, which include monitoring conducted in the following circumstances:
(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3) where the consent of the user of that service has been obtained.
18 U.S.C. ? 3121(b) (2000).

[143] Id. Sec. 2510-2522.

[144] **اضافة المترجم.**

[145] See generally DOJ Manual, supra note 12, at 116-41 (describing protection of the Wiretap Act and its exceptions).

[146] 18 U.S.C. Sec. 3123(a) (3)(A) (Supp. 2002).

[147] See 18 U.S.C. Sec. 2510(21), 2511(2)(i) (Supp. 2002). See generally Kerr, Internet Surveillance, supra note 10, at 658-71.

[148] 18 U.S.C. Sec. 2511(2)(i)(III) (Supp. 2002).

لديه توقع معقول للخصوصية في اتصالاته غير المشروعة، فلا ينبغي مطالبة السلطات بالحصول على أمر لمراقبة اتصالات الهاكر بموافقة الضحية[149].

لا يخلو نهج قانون الطوارئ في المراقبة المستقبلية من عيوبه. العديد من قواعده غير واضحة، وبعضها تمت صياغته بشكل سيئ[150]. ولكن المفهوم الأساسي سليم. حيث تتخذ القواعد خطوة أولى نحو تحديث القانون بحيث يعكس بشكل أفضل الديناميات الجديدة للمراقبة المحتملة لشبكة الحاسوب.

C. اجراء المعمل الشرعي الحاسوبي

C. The Computer Forensics Process

يحتاج اجراء المعمل الشرعي الحاسوبي أيضا إلى نظام من القواعد المصممة خصيصا لتهديدات الخصوصية والاحتياجات التي تثيرها الاستخدامات الحديثة لأجهزة الحاسوب. فمن ناحية، ينبغي أن يحترم القانون القيود التكنولوجية المفروضة على أساليب وتقنيات التفتيش القائمة.

ومن ناحية أخرى، ينبغي أن تنظر القواعد إلى ما هو أبعد من الدينامية التقليدية لتنظيم عمليات التفتيش والضبط لموازنة العبء الذي قد تفرضه هذه القيود التقنية. فعلى سبيل المثال، إذا اقتضت الاحتياجات التقنية إجراء عمليات تفتيش خارج الموقع للحواسيب المضبوطة، فينبغي السماح بإجراءات التفتيش خارج الموقع. لكن القانون لا يجب أن يتوقف عند هذا الحد.

ويمكن تعديل القواعد الفيدرالية للإجراءات الجنائية Federal Rules of Criminal Procedure لمطالبة المحققين investigators بالبدء فورا في تحليل المعمل الشرعي للحواسيب المضبوطة، وإعادة الحواسيب التي لا تحتوي على أدلة في غضون فترة زمنية معقولة. وقد توفر القواعد آلية صريحة تسمح للمشتبه فيهم بالنص على دقة صورة طبق الأصل من حواسيبهم ومن ثم التمتع بالحق في إعادة حواسيبهم في غضون فترة زمنية محددة[151].

قد تتطلب القواعد أيضا أن يقوم المحققون بمسح أية نسخ من الملفات المضبوطة seized files عند إغلاق قضية جنائية، أو على الأقل منع المحققين من فتح أو مراجعة ملفات الحاسوب المضبوطة بعد تلك النقطة

[149] See Orin S. Kerr, Are We Overprotecting Code? Thoughts on First-Generation Internet Law, 57 Wash. & Lee L. Rev. 1287, 1298-1300 (2000) (discussing difficulties created by applying Title III's "one-size-fits-all" approach to variety of internet communications).

[150] For example, existing law does not make clear the precise scope of "contents" versus "DRAS," or even whether there is a third category of communication outside these two categories. Kerr, Internet Surveillance, supra note 10, at 644-48, 645 n.186. It also defines the scope of the trespasser exception using sloppy language. Id. at 667-69.

[151] Of course, exceptions would be required for cases involving computerized contraband such as images of child pornography, as the equipment used to commit child pornography is subject to forfeiture provisions. See 18 U.S.C. Sec. 2253 (2000) (criminal forfeiture); id. Sec. 2254 (civil forfeiture); cf. United States v. Hill, 322 F. Supp. 2d 1081, 1091-92 (C.D. Cal. 2004) (Kozinski, J., by designation) (holding that defendant has right to independent inspection of child pornography evidence, despite government's objections that material should not be allowed to be copied due to potential dissemination).

دون إذن من المحكمة الخاصة. وبشكل عام، ستحاول هذه التغييرات تحقيق التوازن بين احتياجات السلطات والحقوق الفردية في الملكية والخصوصية في ضوء الحقائق التكنولوجية القائمة."[152].

يمكننا أيضا التفكير بشكل خلاق في القواعد التي تنظم عملية الفحص نفسها. وعلى سبيل المثال، تتمثل إحدى طرق التعامل مع مشكلة الإبرة الرقمية في كومة قش في رفض قاعدة العرض العادي في سياق اجراءات التفتيش عن الأدلة الرقمية. وبموجب مبدأ الرؤية الواضحة، يمكن للمحققين مصادرة أدلة لا علاقة لها بالتفتيش عندما يصادفونها في سياق تفتيش صحيح وتظهر طبيعتها المجرمة على الفور.

ونظرا لأنه يجب في كثير من الأحيان تفتيش أجهزة الحاسوب بشكل شامل لتحديد موقع الأدلة المطلوبة، فإن قاعدة الرؤية البسيطة تهدد بانهيار التمييز بين الأوامر الخاصة والعامة. فقد يصبح أمر معين من الناحية النظرية أمرا عاما في الممارسة العملية، حيث قد تظهر جميع الأدلة الموجودة في الحاسوب على مرأى من الجميع أثناء تحليل المعمل الشرعي. ومن شأن إلغاء مبدأ الرؤية البسيطة في اجراءات التفتيش الحاسوبية أن يعالج هذه المشكلة. وسواء أقرتها المحاكم أو صاغها الكونغرس، فإن القاعدة التي تنص على أن الأدلة الرقمية المكتشفة خارج نطاق مذكرة التوقيف غير مقبولة من شأنها أن تقضي على أي حافز لتحويل التفتيش المستهدف إلى رحلة صيد.

في حين لم تحدث أي تغييرات دراماتيكية في المحاكم أو الكونغرس، كانت هناك علامات تغيير مثيرة للاهتمام في المحاكم. بدأ بعض القضاة في إنشاء مجموعة جديدة من قواعد التعديل الرابع المتميزة التي تحاول الاستجابة للتحول من الأدلة المادية إلى الأدلة الإلكترونية. وعدد قليل من هذه التغييرات منتشر بالفعل على نطاق واسع؛ البعض الآخر بدأ للتو في الظهور. بعضها قيم شاذة outliers عند النظر إليها وسط مجموعة القانون ككل. لكن المفتاح هو أن القضاة بدأوا في ثني bend القواعد استجابة للحقائق الجديدة لعملية المعمل الشرعي الحاسوبي. وقد خلص عدد من القضاة إلى أن عمليات التفتيش الحاسوبية "خاصة special"[153]، "فريدة unique"[154]، و"مختلفة different"[155]، ويبحثون عن قواعد جديدة للإجراءات الجنائية تعيد وظيفة القواعد القديمة بالنظر إلى الحقائق الجديدة.

والقاعدة الجديدة الأكثر رسوخا هي أن المحققين قد يقوموا بضبط جهاز الحاسوب الخاص بالهدف ويأخذونه خارج الموقع لمراجعته لاحقا. وعلى الرغم من أن المحاكم لا تتسق إلى حد ما مع القاعدة التقليدية التي تنص على أنه لا يجوز للمحققين ضبط ممتلكات تتجاوز نطاق السبب المحتمل، فقد وافقت المحاكم بشكل موحد على هذه الممارسة على أساس التطبيق العملي. ولقد لاحظ القضاة أن الأمر يستغرق وقتا طويلا ويتطلب الكثير من الخبرة للبحث في جهاز حاسوب في الموقع[156]. وإن ضبط جهاز حاسوب بأكمله يجتاز الحشد الدستوري لأنه "من الناحية العملية، فإن ضبط حاسوب وجميع الأقراص المتاحة وتفتيشه خارج الموقع كان حول أضيق عملية تفتيش وضبط يمكن تحديدها بشكل معقول للحصول على الأدلة"[157]. والبدائل غير عملية،

---

[152] ion). 153. Cf. James M. Rosenbaum, In Defense of the Hard Drive, 4 Green Bag 2d 169, 171 (2001) (suggesting rules that might limit authority of employers to search employee computers, including a time-out period combined with prior notice).
[153] . United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).
[154] United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930, at *4 (D. Utah Apr. 12, 2001).
[155] People v. Gall, 30 P.3d 145, 156 (Colo. 2001) (Martinez, J., dissenting).
[156] See Hill, 322 F. Supp. 2d at 1089-90 (noting time required to search a computer without damaging it).
[157] . United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

وبالتالي فهي غير ملزمة دستوريا. فلن يكون من المعقول "مطالبة مأمور الضبط القضائي بالتدقيق في ... ملفات الحاسوب الموجودة في مكتب المتهم، في محاولة لفصل تلك المواد التي كانت خارج المذكرة"[158].

مثل هذه المخاوف ليست غريبة على التعديل الرابع، بالطبع. فقد سمح جانب المعقولية في التعديل الرابع بمرونة مماثلة في سياقات أخرى أكثر تقليدية[159]. لكن الممارسات تحجرت تدريجيا إلى قاعدة جديدة للتعديل الرابع: مذكرة صالحة تخول المحققين مصادرة أجهزة الحاسوب وتفتيشها خارج الموقع في وقت لاحق.

في حين خففت المحاكم القواعد التقليدية للسماح بالتفتيش خارج الموقع، فقد شدد البعض أيضا القواعد لمحاولة الحد من اجراء المعمل الشرعي وتجنب التفتيش العام في أجهزة الحاسوب المضبوطة. وعلى سبيل المثال، بدأ عدد من قضاة الفيدراليين في إصدار أوامر بتفتيش أجهزة الحاسوب فقط بشرط أن تتبع السلطات قيودا خاصة على التفتيش اللاحق. وقد طالب بعض القضاة السلطات بتفتيش الحاسوب في إطار زمني محدد وإعادة الحاسوب إلى المشتبه به في الوقت المناسب إذا لم يتم العثور على دليل[160].

تشير قضية حديثة من شيكاغو إلى أن بعض القضاة يتخذون خطوات أكثر جرأة[161]. وفي التفتيش عن 3817 دبليو ويست إند، رفض القاضي طلب السلطات للحصول على أمر بتفتيش جهاز حاسوب منزلي ما لم توافق السلطات أولا على الالتزام ببروتوكول التفتيش في الحاسوب المعتمد مسبقا والذي يحدد الخطوات التي سيتم اتخاذها لتحديد موقع الأدلة المخزنة في القرص الصلب[162]. وكان الهدف من التفتيش يشتبه في مشاركته في الاحتيال الضريبي، وأثبت المحققون سببا محتملا للاعتقاد بوجود أدلة على الجريمة على جهاز الحاسوب المنزلي الخاص به. ولقد رفض القاضي السماح بتفتيش جهاز الحاسوب الخاص به دون بروتوكول تفتيش محدد يوافق عليه القاضي، بحجة أن القيام بذلك سيمنح المحققين "ترخيصا للتجول في كل شيء في الحاسوب دون قيود ودون معايير".

وبرر القاضي هذا الشرط بأربعة شواغل عملية: أن الحواسيب تضبط أولا وتفتش في وقت لاحق؛ وحقيقة أن الحواسيب تصادر أولا وتفتش في وقت لاحق؛ واحتمال اختلاط أدلة الجريمة بملفات بريئة وغير ذات صلة؛ حيث حقيقة أن أجهزة الحاسوب يمكنها تخزين كمية هائلة من المعلومات؛ ووجود أساليب تقنية لتحسين

---

[158] United States v. Henson, 848 F.2d 1374, 1383-84 (6th Cir. 1988); see also United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997), aff'd 178 F.3d 1281 (3d Cir. 1999) ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant ... .").

[159] For example, in Illinois v. McArthur, 531 U.S. 326 (2001), the Supreme Court held that the police could seize a man to stop him from entering his home because the police reasonably believed that he was going to destroy evidence inside and the police were in the process of obtaining a warrant. According to the Court, the seizure of the man was permissible because "[i]t involve[d] a plausible claim of specially pressing or urgent law enforcement need, i.e., 'exigent circumstances.'" Id. at 331.

[160] According to the DOJ Manual: Several magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time. DOJ Manual, supra note 12, at 77.

[161] In re Search of 3817 W. West End, 321 F. Supp. 2d. 953 (N.D. Ill. 2004).

[162] Id. at 955-56.

عمليات التفتيش[163]. وفي ضوء هذه المخاوف العملية، استنتج القاضي أن شرط الخصوصية أجبر على الموافقة المسبقة على أساليب التفتيش لضمان أن يكون التفتيش معقولا دستوريا."[164].

كما غيرت المحاكم القواعد التي تراقب عندما يتجاوز التفتيش نطاق الأمر. لم تقم أية محكمة بإلغاء قاعدة الرؤية الواضحة تماما، لكن محكمتين على الأقل ضيقتها في الممارسة العملية من خلال التركيز على النية الذاتية للمحقق. والقاعدة العامة هي أن نية الضابط الذاتية في الانحراف خارج الأمر لا يهم. وكما ذكر آنفا، فإن هذه القاعدة تجعل من الصعب على المحاكم معرفة ما إذا كان التفتيش الحاسوبي مصمما بشكل ضيق[165]. ففي قضية United States v. Carey، كان المحقق يفتش في القرص الصلب المضبوط عن أدلة تتعلق بالكوكايين، صادف صورا لاستغلال الأطفال في المواد الإباحية. وتوقف المحقق عن التفتيش عن الأدلة المتصلة بالمخدرات وقضى الساعات القليلة التالية في البحث عن صور لاستغلال الأطفال في المواد الإباحية[166].

وقضت الدائرة العاشرة بأن النية الذاتية للضابط تحكم: ولأن الضابط غير تركيز تفتيشه من نوع إلى آخر من الأدلة، فإن اكتشاف الأدلة خارج نطاق الأمر غير مسموح به وتم رفض الأدلة[167]. وبالمثل، في قضية United States v. Gray. غراي، وهو محقق يفتش في قرص صلب تم الاستيلاء عليه عملا بأمر للحصول على أدلة على اختراق الحاسوب computer hacking، صادف صورة لاستغلال الأطفال في مواد إباحية child pornography [168]. وواصل المحقق التفتيش عن أدلة الاختراق، لكنه لاحظ صورا إضافية لاستغلال الأطفال في المواد الإباحية اكتشفها على طول الطريق[169]. أيدت المحكمة مقبولية استغلال الأطفال في المواد الإباحية، معتبرة أن النية الذاتية للمحقق أبقت التفتيش في نطاق الأمر[170].

بموجب كاري وجراي، فإن قاعدة الرؤية البسيطة لها حد جديد في حالات الحاسوب: فهي تسمح بضبط على الأدلة خارج المذكرة فقط إذا تم الكشف عنها وفقا للتفتيش بحسن نية عن الأدلة الموضحة في المذكرة. تحاول القاعدة الجديدة استعادة بعض وظائف القاعدة القديمة بالنظر إلى الحقائق الجديدة لعملية المعمل الشرعي للحاسوب.

---

[163] Id. at 962.
[164] Id. at 958-59.
[165] Other courts have suggested similar approaches. See, e.g., United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (suggesting that magistrate judge's authorization of search supported by affidavit that explained need for off-site search of computer constituted "the magistrate judge's authorization" of off-site search); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000) (suggesting that magistrate judge should approve search strategy for search of a computer); People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (Martinez, J., dissenting) (arguing for a new Fourth Amendment rule governing search of computers "to properly protect privacy concerns inherent in the complex nature of computers"). Of course, these approaches are somewhat difficult to square with traditional doctrine. That doctrine requires the government to specify the place to be searched and the item for which to search, but traditionally has not been understood as requiring an explanation of how the search is to be executed.
[166] See supra notes 90-92 and accompanying text.
[167] 172 F.3d 1268, 1271 (10th Cir. 1999).
[168] Id. at 1274.
[169] 78 F. Supp. 2d 524 (E.D. Va. 1999).
[170] Id. at 527.

الخلاصة

CONCLUSION

غالبا ما تؤدي التغييرات في التكنولوجيا إلى تغييرات في القانون. حيث تتطور القواعد القانونية استجابة للتغيرات في الحقائق الأساسية. ونظرا لاعتمادنا الشديد على الحواسيب والطرق المحددة التي تعمل بها، فإن استخدام الحواسيب في النشاط الإجرامي يشكل تحديات كبيرة للقواعد التقليدية للإجراءات الجنائية. وبالاستعاضة عن جمع الأدلة الرقمية بجمع الأدلة المادية وإفادات شهود العيان، تحل التحقيقات التي تنطوي على حواسيب محل الآليات التقليدية للتفتيش والضبط بأشكال مختلفة تماما من المراقبة وأشكال جديدة من تحليل المعمل الشرعي. ومن الطبيعي أن يتغير القانون ردا على ذلك.

وعلى الرغم من أن بعض التغييرات ستأتي من المحاكم في شكل تطور بطيء للقواعد العقائدية، إلا أن البعض الآخر يجب أن يتبع إعادة التفكير في أفضل القواعد لتنظيم الجمع الرقمي digital collection وأفضل المؤسسات لإنشاء وتنفيذ تلك القواعد. حيث يجب أن تلهم مشكلة الأدلة الرقمية إنشاء إجراء جنائي جديد، وهو مجموعة من القواعد التي تبني على الحلول التقليدية وتتوسع منها لتبني آليات جديدة ومبتكرة لتنظيم جمع الأدلة واستخدامها.

يجب أن ندرك أيضا أن مشكلة الأدلة الرقمية تمتد إلى ما وراء حدودنا، وأنه يمكن العثور على حلول ورؤى مفيدة هناك. تمر كل دولة صناعية بنفس التحولات من الأدلة المادية وشهادات شهود العيان إلى الأدلة الرقمية التي تحدث في الولايات المتحدة. نستخدم جميعا نفس الشبكات ونفس الأجهزة ونفس البرامج. على الرغم من أن البلدان المختلفة لديها تقاليد دستورية مختلفة وتحمي قيما مختلفة، إلا أنها تواجه جميعها نفس الأسئلة الأساسية حول كيفية تنظيم جمع الأدلة من طرف ثالث، والمراقبة المستقبلية، واجراء المعمل الشرعي الحاسوبي. من خلال البحث على نطاق واسع عن ترتيبات ومناهج مؤسسية جديدة لتنظيم جمع الأدلة الرقمية، يمكننا أن نفتح أنفسنا لأفضل الأفكار في الخارج لاستكمال الحلول الناتجة عن تقاليدنا الدستورية.

قوانين العالم الافتراضي

The Laws of Cyberspace

لورانس ليسيج

Lawrence Lessig

قبل الثورة، كان لدى روسيا القيصرية نظام داخلي لجوازات السفر internal passport . وكان الناس قد كرهوا هذا النظام وتميز هذه الجوازات الحوزة التي جئت منها، حيث تحدد علامة الأماكن التي يمكن أن تذهب اليها وترتبط بها. كانت جوازات السفر شارات تتيح الوصول، أو منع الوصول. وبذا تمت السيطرة على ما في الدولة الروسية حيث يمكن للروس أن يأتوا لمعرفة السلوك في العالم الفعلي- هذا العالم، العالم الذي أنا أتحدث منه الآن- تم تنظيمه من قبل أربعة أنواع من القيود. القانون هو واحد من تلك القيود الأربعة. القانون ينظم العقوبات بطريقة سابقة على الواقعة imposed ex post - كالفشل في دفع الضرائب الخاصة بك، وكنت من المرجح أن تذهب إلى السجن، ولكن سرقة سيارتي، وأنت أيضا من المحتمل أن تذهب إلى السجن. القانون هو البارز ممن يتولى التنظيم. لكنه واحد من أربعة فقط.

فقد وعد البلاشفة Bolsheviks بتغيير كل هذا. كما وعدوا بإلغاء جوازات السفر الداخلية. ولاحقاً عند وصولهم إلى السلطة فعلوا ذلك تماما. الروس كانوا أحراراً مرة أخرى في السفر حيث تمنوا. ولم يتم تحديد المكان الذي يمكن أن تذهب اليه من قبل بعد الوثيقة التي كان مطلوبا منهم أن تحمل معهم. فإلغاء جواز السفر الداخلي يرمز إلى حرية الشعب الروسي– فتم ارساء ديمقراطية المواطنة في روسيا.

بيد أن هذه الحرية لم تكن لتدوم. وبعد عقد ونصف العقد، وفي مواجهة احتمال إغراق الفلاحين جوعاً في المدن بحثاً عن الغذاء، أعاد ستالين نظام جوازات السفر الداخلية. وربط الفلاحون مرة أخرى بأراضيهم الريفية (وهو قيد ظل طوال السبعينات). ومرة أخرى تم تقييد الروس بما يسمح به جواز سفرهم. مرة أخرى، للوصول إلى روسيا، كان على الروس أن يظهروا شيئاً عن من هم.

* * *

السلوك Behavior في العالم الحقيقي- هذا العالم، العالم الذي أنا أتكلم الآن- وينظم من قبل أربعة أنواع من القيود. القانون هو واحد من تلك القيود الأربعة. القانون ينظم بالعقوبات فرض السابقين بعد -- تفشل في دفع الضرائب الخاصة بك، وكنت من المرجح أن تذهب إلى السجن، ولكن سرقة سيارتي، وأنت أيضا من المحتمل أن يذهب إلى السجن. القانون هو بارزة من المنظمين. لكنها واحدة من أربعة.

المعايير الاجتماعية Social norms هي الثانية. كما أنها تنظم. فالمعايير الاجتماعية- هي تفاهمات understandings أو توقعات expectations حول كيفية يجب أن تتصرف، اكراه enforced ليس من خلال بعض معيار مركزي ملزم، ولكن بدلا من ذلك من خلال التفاهمات والتوقعات من الجميع تقريبا داخل مجتمع معين– مباشر وبتقييد سلوكي في مجموعة أوسع بكثير من السياقات من أي قانون. اذ تقرر المعايير نوعية الملابس سوف أرتدي- بدلة، وليس رداء؛ يقولون لك أن تجلس بهدوء، وبأدب، لمدة 40 دقيقة على الأقل بينما أتكلم، وهم يقومون بتنظيم كيف أننا سوف تتفاعل بعد هذا انتهاء هذا الحديث. فالمعايير دليل السلوك; وبهذا المعنى، فإنها تعمل كقيد تنظيمي ثانٍ.

السوق هو قيد constraint ثالث. ينظم حسب السعر. السوق يحد من المبلغ الذي يمكن أن تنفق على الملابس; أو المبلغ الذي يمكنني أن أجنيه من الخطب العامة؛ يقرر أنني أستطيع أن اطلب أقل لكتاباتي من مادونا، أو أقل لغنائي من بافاروتي. ومن خلال جهاز السعر، يحدد السوق فرصي، ومن خلال هذا النطاق من الفرص، يتولى التنظيم.

وأخيراً، هناك قيد على ما يمكن أن يسميه البعض الطبيعة، والذي أريد تسميته بـ.. "الهندسة المعمارية architecture". هذا هو قيد العالم كما أجده، حتى لو كان هذا العالم كما أجد أنه عالم صنعه الآخرون. أن لا أستطيع أن أرى من خلال هذا الجدار هو قيد على قدرتي على معرفة ما يحدث على الجانب الآخر من الغرفة. عدم وجود منحدر وصول إلى مكتبة يقيد وصول واحد مقيد إلى كرسي متحرك. هذه القيود، بالمعنى الذي أعنيه هنا، تنظم. ولفهم التنظيم *regulation*، يجب أن نفهم مجموع هذه القيود الأربعة التي تعمل معا. ولا يمكن لأي واحد بمفرده أن يمثل أثر الأربعة معاً.

* * *

هذا هو عصر التحررية الافتراضية cyber-libertarian. فهو وقت اشتعلت فيه بعض الضجة حول العالم الافتراضي cyberspace. فالضجيجhype يذهب مثل هذا: العالم الافتراضي أمر لا مفر منه Cyberspace is unavoidable، ويعد العالم الافتراضي الان غير قابل للتنظيم cyberspace is unregulable. ولا يمكن لأي دولة أن تعيش بدونه، ومع ذلك لن تتمكن أية دولة من السيطرة على السلوك فيه. فالعالم الافتراضي هو ذلك المكان الذي يكون فيه الأفراد، بطبيعتهم، متحررين من سيطرة السيادة sovereigns الحقيقية. فهو، على حد تعبير جيمس بويل James Boyle ، تكنو كبير"gotcha" - لأمم العالم، لا يمكنك أن تعيش بها، ولكن أمم العالم، فحالما تحصل عليه، فلن تعيش طويلا معه.

هدفي اليوم هو وجهة نظر مختلفة حول العالم الافتراضي. هدفي هو مهاجمة هذه الضجة. ذلك أن العالم الذي ندخله في رأيي ليس عالما من الحرية الدائمة perpetual freedom؛ بل هو عالم من الحرية الدائمة. أو بتعبير أدق، العالم الذي ندخله ليس عالماً تكون فيه الحرية مضمونة freedom is assured. إن العالم الافتراضي لديه القدرة على أن يكون أكثر الأماكن تنظيماً، وعلى نطاق واسع، الذي عرفناه على الإطلاق- في أي مكان وفي أي وقت من تاريخنا. لديه القدرة على أن يكون نقيض مساحة من الحرية. وما لم نفهم هذه الإمكانية، وما لم نرى كيف سيكون ذلك، فمن المرجح أن ننام خلال هذا الانتقال من الحرية إلى السيطرة. لذلك، في رأيي، هو الانتقال الذي نشهده الآن.

والآن أريد أن أسوق هذه الحجة باستخدام المقدمتين اللتين بدأتهما اليوم- وهما القصة عن روسيا البلشفية، والفكرة المتعلقة بالتنظيم. لأنها سوف توحي معا حيث العالم الافتراضي هو الذهاب، والأهم من ذلك، كيف فقط نحن يمكن أن نتوقع العالم الافتراضي للوصول الى هناك.

الفكرة الأولى: تماما كما هو الحال في العالم المادي، يتم تنظيم السلوك في العالم الافتراضي من قبل أربعة أنواع من القيود. والقانون هو مجرد أحد تلك القيود. على الرغم من الضجيج، هناك قانون واحد فقط الآن في العالم الافتراضي- قانون حقوق الطبع والنشر copyright law، أو قانون السب والقذف والتشهير defamation law، أو قانون التحرش الجنسي sexual harassment law، وكلها تقيد السلوك في العالم الافتراضي بنفس الطريقة التي تقيد السلوك في العالم المادي.

و هناك أيضا، وربما من المدهش جدا، معايير في العالم الافتراضي- هي القواعد التي تحكم السلوك، وتعرض الأفراد لعقوبة من الآخرين. وهي تعمل أيضا في العالم الافتراضي حيث تعمل المعايير في العالم المادي، وتهدد العقوبات اللاحقة من قبل المجتمع threatening punishments ex post by a community.

وكذلك مع السوق. السوق يقيد ما في العالم الافتراضي، تماما كما هو الحال في العالم المادي. تغيير سعر الوصول، والقيود على الوصول تختلف. تغيير هيكل تسعير الوصول structure of pricing access، وتنظيم الوصول الهامشي regulation of marginal access التحولات بشكل كبير shifts dramatically أيضا.

ولكن لأغراضنا هنا، فإن أهم هذه القيود الأربعة على السلوك في العالم الافتراضي هو القياس/التناظرية analog لما أسميه الهيكلة *architecture* في العالم/ المادي الحقيقي: هذا سوف أسميه البرمجة *code*. وبالبرمجة، أعني ببساطة البرمجيات software والأدوات/ العتاد hardware التي تشكل العالم الافتراضي كما هو- مجموعة البروتوكولات set of protocols، ومجموعة القواعد set of rules، التي تطبق implemented، أو المقننة codified، في برنامج العالم الافتراضي نفسه، والتي تحدد كيفية تفاعل الناس، أو وجودهم، في هذا العالم. هذا الرمز، مثل الهندسة المعمارية في العالم المادي الحقيقي، يحدد الشروط حال الدخول عليها، أو موجودة في العالم الافتراضي. انها، مثل الهندسة المعمارية، ليست اختيارية. فأنا لا اختار ما إذا كان على طاعة الهياكل التي ينشئها – او كما حين يختار الهكرة، ولكن الهكرة لهم وضع خاص. بالنسبة للبقية منا، والحياة في العالم الافتراضي تخضع للبرمجة، تماما كما الحياة في العالم المادي الحقيقي حيث تخضع لبنية العالم الحقيقي.

وتختلف جوهر قيود البرمجة في العالم الافتراضي. فما توصلوا اليه من خبرات لا تختلف. وفي بعض الأماكن، يجب على المرء إدخال كلمة مرور password قبل أن يحصل أي أحد على الدخول; وفي أماكن أخرى، يمكن للمرء أن يدخل سواء تم تحديدها أم لا. وفي أماكن اخرى، تنتج المعاملات التي يُشرك فيها الشخص آثاراً تربط المعاملات بالفرد؛ وفي أماكن أخرى، يتم لا يتم تحقيق هذا الرابط إلا إذا اختار الفرد. في البعض الاخر من الأماكن، يمكن للمرء أن يختار التحدث بلغة تتيح للمستلم فقط سماعها (من خلال التشفير)؛ وفي أماكن أخرى، التشفير ليس خيارا.

وتشكل الاختلافات differences من قبل رمز هذه الأماكن المختلفة. التعليمات البرمجية code أو البرمجيات software أو الهيكلة architecture أو بروتوكولات protocols هذه المسافات تعيين هذه الميزات; فهي ميزات تم تحديدها بواسطة كتّاب التعليمات البرمجية code writers؛ أنها تقيد بعض السلوك بجعل سلوك آخر ممكن. وبهذا المعنى، فإنهم، مثل العمارة في العالم الحقيقي، ينظمون السلوك في العالم الافتراضي.
البرمجة والأسواق والقواعد والقانون معا تتولى كلها التنظيم في العالم الافتراضي ثم كما الهيكلة والسوق والمعايير والقانون تتولى التنظيم في الفضاء الحقيقي. وادعائي هو أنه كما هو الحال مع تنظيم العالم المادي الحقيقي، ينبغي أن ننظر في كيفية عمل هذه القيود الأربعة معا.

ومن الأمثلة على ذلك- التناقض contrast بين التنظيم في العالم المادي الحقيقي، والتنظيم نفسه في العالم الافتراضي- أن يوضح هذه النقطة بشكل أكثر وضوحا. فكروا في القلق concern في بلدي (قد يسميه البعض هاجس obsession) مع تنظيم الفحشاء indecency على الشبكة net.

وقد انطلق هذا القلق في الولايات المتحدة في أوائل عام 1995. كان مصدره ارتفاعًا استثنائيًا في عدد المستخدمين العاديين للنت، وبالتالي ارتفاعًا في الاستخدام من قبل الأطفال، وارتفاعًا أكثر استثنائية في توافر ما يسميه الكثيرون "الإباحية porn" على الشبكة. ذكرت دراسة مثيرة للجدل للغاية (ومعيبة بشكل أساسي fundamentally flawed) نشرت في مجلة Georgetown University Law Review في جامعة

جورجتاون وقررت أن الشبكة تعج بـ الإباحية. ولقد نرت كل من مجلة التايم Time ونيوزويك Newsweek على حد سواء مقالات تغطي قصص حول توافرها. كما تعرض أعضاء مجلس الشيوخ وأعضاء الكونغرس للقصف بمطالب للقيام بشيء ما لتنظيم "الصوت الافتراضي cybersmut".

لماذا كان هذا الغضب كبيرًا جدًا حول الإباحية في العالم الافتراضي. وبالتأكيد، يوجد المزيد من الإباحية في العالم الحقيقي مما هو عليه في العالم الافتراضي. فلماذا الغضب حول الوصول إلى الإباحية في مكان لا يملك معظم الأطفال الوصول إليه؟

ولفهم السبب، والتفكير لثانية واحدة حول نفس المشكلة كما هو موجود في العالم الحقيقي. ما الذي ينظم توزيع الإباحية في العالم الحقيقي؟

أولاً: في أمريكا، تنظم القوانين في العالم الحقيقي توزيع الإباحية على الأطفال- القوانين التي تتطلب من بائعي الإباحية التحقق من عمر المشترين، أو القوانين التي تتطلب أن يقع البائعون في قسم من المدينة من المرجح أن يكونوا بعيدين عن الأطفال. ولكن القوانين ليست أهم القيود المفروضة على توزيع الإباحية على الأطفال.

والأكثر أهمية من القوانين هي المعايير. تقيد المعايير البالغين بعدم بيع الإباحية للأطفال. حتى بين الموزعين الاباحية هذا القيد فعال نسبيا.

وليس فقط المعايير الاجتماعية. السوق أيضا، فالأفلام الاباحية تكلف المال، والأطفال ليس لديهم المال.

لكن أهم قيد على المساحة الحقيقية هو ما أسميتُه الهيكلة *architecture*. لكل هذه التنظيمات regulations الأخرى في العالم الحقيقي تعتمد على هذا القيد من الهيكلة. فالقوانين والمعايير والسوق يمكن التمييز ضد أنواع في الفضاء الحقيقي، لأنه من الصعب في العالم الحقيقي إخفاء أنك طفل. وبالطبع، يمكن للطفل ارتداء شارب، والوضع على ركائز متينة، والمحاولة لدخول متجر الاباحية لشراء الاباحية. لكن في الغالب، التنكر سوف يفشل. في معظم الأحيان، سيكون من الصعب جداً إخفاء أنه طفل. وهكذا، وفي معظم الأحيان، القيود القائمة على كونه طفلا هي القيود التي يمكن أن تكون فعالة.

والعالم الافتراضي مختلف. حتى لو افترضنا أن نفس القوانين تنطبق على العالم الافتراضي كما هو الحال في العالم الحقيقي، وحتى لو افترضنا أن قيود المعايير والسوق قد تم ترحيلها أيضا، وحتى مع ذلك، لا يزال هناك فرق حاسم بين العالمين.

لأنه بينما في العالم الحقيقي من الصعب إخفاء أنك طفل، فانه في العالم الافتراضي، فان إخفاء من أنت/ ماهيتك، أو بتعبير أدق، إخفاء الميزات حول من أنت هو أبسط شيء في العالم. والفرض في العالم الافتراضي هو الاخفاء/ عدم الكشف عن الهوية anonymity. ولأنه من السهل جدا إخفاء الماهية، فمن المستحيل عمليا للقوانين، والمعايير، ان تطبق في العالم الافتراضي. لتطبيق هذه القوانين، يجب على المرء أن يعرف أنه هو طفل واحد يتعامل معه. ولكن بنية العالم الافتراضي ببساطة لا توفر هذه المعلومات.

الآن النقطة الهامة هي أن نرى الفرق، وتحديد مصدره. والفرق هو الاختلاف في ما أريد أن أسميه إمكانية التراجع في العالم الافتراضي- قدرة الحكومات على تنظيم السلوك هناك. وكما هو الحال الآن، فإن العالم الافتراضي هو مساحة أقل قابلية للانكسار من العالم الحقيقي. هناك أقل ما يمكن أن تفعله الحكومة.

مصدر هذا الاختلاف في القابلية للتنظيم regulability هو اختلاف في بنية العالم- وهو اختلاف في تعليمات البرمجة التي تشكل العالم الافتراضي كما هو. هيكلته، وادعي هو، يجعله غير قابلة للتنظيم أساسا.

أو هكذا فعلت في عام 1995، وفي عام 1996، عندما قام الكونغرس الأميركي في نهاية المطاف بتمرير محاولة لمعالجة هذه المشكلة- قانون آداب الاتصالات the Communications Decency Act. سوف أتحدث قليلاً عما حدث لذاك التشريع statute ، لكنني أريد أولاً أن أحتفل بهذه الفترة، وأنطلق من حيث نحن اليوم. وكان هيكل العالم الافتراضي في عام 1995، و 1996 قد جعل من غير تنظيم أساسا.

دعونا نستدعي هيكلة الشبكة Net 95 — كما في عام 1995 — وهنا ملامحها: طالما كان لدى المرء إمكانية الوصول إلى Net95، يمكن للمرء أن يتجول دون تحديد من هو. كانت شبكة Net95 تمثل روسيا البلشفية. كانت هوية المرء، أو ميزاته، غير مرئية للنت في ذلك الوقت، حيث يتمكن المرء من الدخول، واستكشاف، بدون أوراق اعتماد بدون جواز سفر داخلي. وكان الوصول مفتوحاً وشاملاً، وليس مشروطاً ببيانات الاعتماد. لقد كانت، بالمعنى الضيق للمصطلح، لحظة ديمقراطية غير عادية. كان المستخدمون متساوين بشكل أساسي. مجاناً بشكل أساسي.

وعلى هذه الخلفية- على خلفية الشبكة كما كانت- شبكة Net95- حيث نظرت المحكمة العليا آنذاك في قانون آداب الاتصالات. وقد قصمت محكمتان أدنى درجة التشريع باعتباره انتهاكاً للحق في حرية التعبير. وفيما شاهد الملايين المحكمة تنظر في الحجج حول القضية- شاهد في العالم الافتراضي، كما تم نشر الحجج، ومناقشتها، ونقدها.

وفي حزيران/يونيه، من العام الماضي، أكدت المحكمة قرار المحاكم الأدنى درجة، حيث قضت بعدم دستورية التشريع. ولكن سببية عدم الدستورية ليست مهمة جدا لأغراضنا هنا. المهم هو الخطاب الذي يقود المحكمة إلى نتائجها.
وبالنسبة للقرار فهو معلق بشكل حاسم على المطالبات حول بنية الشبكة كما على- على الهيكلة، وهذا من شبكة Net95. وبالنظر إلى أن الهيكلة، وكما خلصت المحكمة، فإن أي تنظيم لمنطقة الأطفال من الاباحية سيكون التنظيم الذي كان مرهقا للغاية على المتكلمين والمستمعين. وكما كانت الشبكة، فإن التنظيم سيكون مرهقاً للغاية.

ولكن ما كان هاما هو أن المحكمة تحدثت كما لو أن هذا الهيكل من الشبكة كما كان- شبكة Net 95 - هو الهيكلة الوحيدة التي يمكن أن تكون كذلك. وقرر انه كما لو كان قد اكتشف طبيعة الشبكة، وبالتالي كان يقرر طبيعة أي امكانية التنظيم للشبكة.

ولكن المشكلة مع كل هذا، بطبيعة الحال، هو أن الشبكة ليس لها طبيعة. لا يوجد بنية واحدة ضرورية لوضع تصميمها. فشبكة Net95 هي مجموعة من الميزات، أو البروتوكولات، التي شكلت شبكة في فترة واحدة من الزمن. ولكن لا شيء يتطلب أن هذه الميزات، أو البروتوكولات، تشكل دائما شبكة كما ستكون دائما. وبالفعل، لا شيء في ما رأيناه في العامين الماضيين يجب أن يقودنا إلى التفكير في أنه سوف تكون كذلك.

مثال قد يجعل هذه النقطة أكثر بساطة. قبل أن أكون أستاذاً في جامعة هارفارد، قمت بالتدريس في جامعة شيكاغو. إذا أراد المرء الوصول إلى الشبكة في جامعة شيكاغو، فانه ببساطة تقوم بتوصيل آلة واحدة إلى الرافعات jacks الموجودة في جميع أنحاء الجامعة. أية آلة يمكن أن تكون متصلة بتلك الرافعات، وبمجرد

الاتصال، سوف يكون لاية آلة حق الوصول الكامل إلى الإنترنت. كان الوصول مجهول الهوية، وكاملاً، ومجانياً.

وكان سبب هذه الحرية هو قرار اتخذته الإدارة. بالنسبة لعميد جامعة شيكاغو هو جيوف ستون Geof Stone، العميد السابق لكلية الحقوق بجامعة شيكاغو، وفقيه بارز في حرية التعبير. عندما كانت الجامعة تقوم بتصميم شبكتها, سأل الفنيون technicians العميد عما إذا كان مسموح باتّصالات مجهولة. وقال العميد، مستشهدا بمبدأ مفاده أن القواعد التي تنظم الخطاب في الجامعة ستكون وقائية لحرية التعبير مثل التعديل الأول، نعم: للشخص الحق في التواصل في الجامعة دون الكشف عن هويته، لأن التعديل الأول للدستور يضمن نفس الحق تجاه الحكومة. من هذا القرار السياسي تدفق هيكل شبكة جامعة شيكاغو.

في جامعة هارفارد، القواعد مختلفة. لا يمكن للمرء أن يربط آلة واحدة إلى الشبكة في جامعة هارفارد ما لم يتم تسجيل آلة—ويتم ترخيصها، والموافقة عليها، والتحقق من ذلك. ويمكن لأعضاء المجتمع الجامعي فقط تسجيل الآلات الخاصة بهم. وبمجرد تسجيلها، يمكن رصد جميع التفاعلات مع الشبكة وتحديدها على جهاز معين. والواقع أن الكلام المجهول على هذه الشبكة غير مسموح به- فهو ضد القواعد. ويمكن التحكم في الوصول على أساس ماهية الشخص; ويمكن تتبع التفاعل، استنادا إلى ما قام به شخص ما.

يرجع سبب هذا التصميم أيضًا إلى قرار المدير administrator- على الرغم من أن المدير هذه المرة أقل تركيزًا على حماية التعديل الأول. فالسيطرة على الوصول هو المثل الأعلى في جامعة هارفارد. وكان تسهيل الوصول مثالي في شيكاغو، ولكن ولذلك تم اختيار التكنولوجيات التي تجعل السيطرة control ممكنة في جامعة هارفارد؛ والتقنيات التي تسهل facilitate الوصول إلى اختيار في شيكاغو.
الآن هذا الفرق بين الشبكتين شائع جدا اليوم. الشبكة في جامعة شيكاغو هو هيكلة للإنترنت في عام 1995. وهو، مرة أخرى، شبكة Net95. ولكن الهيكلة في جامعة هارفارد ليست بنية إنترنت internet architecture. بل هي بنية إنترانت intranet architecture. والفرق هو ببساطة هذا- وهو أن الهوية في شبكة إنترانت، تُرسَل بما فيه الكفاية بحيث يمكن التحكم في الوصول، ورصد الاستخدام. البروتوكولات الأساسية لا تزال TCP/IP— بمعنى البروتوكولات الأساسية أو الأساسية للإنترنت. ولكن المراتب layered على رأس هذا البروتوكول الأساسي هو مجموعة من البروتوكولات التي تسهل السيطرة. شبكة هارفارد هي الإنترنت مضاعفة internet plus، حيث زائد plus يعني القدرة على السيطرة.

تعكس هاتان البنياتان فلسفتان حول الوصول access. وهي تعكس مجموعتين من المبادئ، أو القيم، حول كيفية السيطرة على الكلام. كما إنها توازي، كما أود أن أقرر، الفرق بين الأنظمة السياسية الحرة political regimes of freedom ، والأنظمة السياسية ذات السيطرة political regimes of control. فهم يتتبعون الاختلاف في الإيديولوجية difference in ideology بين ألمانيا الغربية وألمانيا الشرقية؛ وبين الولايات المتحدة وجمهورية الاتحاد السوفياتي السابق؛ وبين جمهورية الصين، والبر الرئيسي للصين. فهي تقف على الاختلاف بين السيطرة والحرية- وهي تظهر هذا الاختلاف من خلال الهيكلة أو تصميم تعليمات البرمجة. وفي هذه الهيكلة تمكن القيم السياسية. وهي اي الهيكلة بهذا المعنى سياسية.

الآن أنا لا أعرض هذا المثال لكي أنتقد هارفارد. هارفارد مؤسسة خاصة; وهي حرّة، في مجتمع حر، وتقرر تخصيص مواردها كيفما ترى. فوجهة نظري بدلا من ذلك هي ببساطة لكي يتحصل القارئ على رؤية تعدد الهياكل العمارات كثيرة، وبالتالي فان كيفية اختيار واحد هو شأن سياسي. وكيف، على مستوى الأمة، ان الهيكلة هي بطبيعتها سياسية. وفي مساحة العالم الافتراضي، واختيار الهيكلة لا يقل أهمية عن اختيار الدستور. وبمعنى أساسي، فان برمجة العالم الافتراضي هو دستوره. وهو يحدد الشروط التي يمكن

للأشخاص الوصول إليه؛ فهو يضع القواعد؛ ويتحكم في سلوكها. وبهذا المعنى، فهي سيادة خاصة. سيادة بديلة alternative sovereignty، تتنافس مع السيادة sovereigns في العالم المادي، في تنظيم السلوك من قبل مواطني العالم المادي.

ولكن المحكمة العليا في الولايات المتحدة تعاملت مع مسألة الهيكلة كما لو تم منح بنية لهذا للعالم الافتراضي. وتتكلم كما لو كان هناك تصميم واحد فقط للعالم الافتراضي- التصميم الذي كان عليه.

وفي هذا الصدد، فإن المحكمة العليا ليست وحدها. وفي رأيي أن أكبر خطأ من منظري العالم الافتراضي theorists of cyberspace- من النقاد، وخاصة المحامين lawyers الذين يفكرون في التنظيم في هذا المجال- هو هذا الخطأ الذي تعتمده المحكمة العليا. إنه خطأ الطبيعة naturalism كما هو مطبق على العالم الافتراضي. فهو خطأ التفكير في أن الهيكلة كما لدينا هي هيكلة التي سيكون لدينا دائمًا؛ أن الفضاء سيضمن لنا الحرية، أو الحرية؛ أنه من الضرورة تعطيل الحكومات التي تريد السيطرة.

وهذا الرأي خاطئ تماما. خطأ عميق Profoundly mistaken لأنه في حين نحتفل الحرية "المتأصلة inherent" من الشبكة، وهيكلة الشبكة تتغير من تحتنا. فالهيكلة تتحول من هندسة الحرية إلى بنية السيطرة. وهي تتحول بالفعل من دون تدخل الحكومة، على الرغم من أن الحكومة سرعان ما تأتي لترى كيف قد تتدخل لتسريعها. وحيث تتدخل الحكومة الآن، فإنها تتدخل بطريقة مصممة لتغيير نفس هذه العمارة - لتغييرها إلى بنية للسيطرة، لجعلها، كما قلت، أكثر قابلية للتراجع. في حين أن النقاد يعدون بالحرية الدائمة المضمنة في بنية الشبكة نفسها، فإن الفنيين والسياسيين يعملون معًا لتغيير تلك الهيكلة، لإبعادها عن بنية الحرية هذه. كمنظرين theorists للعلم الافتراضي، يجب أن نفهم هذا التغيير. ويجب أن نعترف بالعواقب السياسية لهذا التغيير. ويجب أن نتحمل المسؤولية عن هذه العواقب. لمسار التغيير لا لبس فيه، وثمرة هذا المسار، السم poison.

وكدستوريين constitutionalists، أن نواجه confront مسألة دستورية أساسية fundamentally constitutional question: إذا كان هناك خيار بين هياكل السيطرة control وهيكلة الحرية architectures of freedom، فكيف نقرر هذه المسائل الدستورية؟ إذا كانت الهياكل كثيرة، ثم ان الدستور ذاته ليس بدليل لنا في اختيار هذه الهياكل؟

وفي رأيي أن القيم الدستورية constitutional values تُورِط بنية العالم الافتراضي. وفي رأيي أيضا، ينبغي للقيم الدستورية أن توجهنا في تصميمنا لهيكلة العالم الافتراضي. وفي رأيي مرة ثالثة، يجب أن تحد القيم الدستورية من أنواع التراجع التي تسمح بها هذه الهيكلة.

ولكن رأيي غائب في التفكير في دور الحكومة في العالم الافتراضي. وفي الواقع، أصبحت أمتي- لسنوات عديدة رمز الحرية في العالم الذي كانت هذه الحرية نادرة فيه- رائدة في دفع بنية الإنترنت من هندسة للحرية إلى بنية للسيطرة. من العمارة، أي التي اعتنقت تقاليد الحرية التي عبر عنها في ماضينا الدستوري، إلى العمارة التي هي في الأساس لعنة لتلك التقاليد.

لكن كيف؟ كيف يمكن للحكومة إجراء هذه التغييرات؟ كيف يمكن للحكومة أن تؤثر على هذه السيطرة؟ لا يستطيع الكثيرون أن يروا كيف يمكن للحكومة أن تؤثر على هذه السيطرة. لذا في الدقائق القليلة المتبقية في حديثي اليوم، أريد أن أريك كيف. أريد أن أرسم لك طريقاً من حيث نحن إلى حيث أخشى أننا ذاهبون أريدك أن ترى كيف يمكن لهذه التغييرات وكيف يمكن للحكومة أن تساعد في جعلها دائمة.

ثم ارجع معي إلى الفكرة التي بدأت في هذا المقال- النقطة المتعلقة بمختلف طرائق التقييد- ولاحظ شيئا مهما بشأن تلك الفكرة لم نلاحظه حتى الآن. لقد قلت في البداية إننا ينبغي أن ننظر إلى القانون باعتباره مجرد واحد من أربع طرائق للقيد modalities of constraint؛ أنّ نحن يجب ان نفكّر فيه أنّ هو فقط جزء واحد من بنية القيد التي يمكن أن تنظّم.

وقد يعتبر المرء ذلك حجة حول تفاهة القانون. وإذا كانت قوى كثيرة أخرى غير القانون تنظم، فإن هذا قد يوحي بأن القانون نفسه لا يمكن أن يفعل سوى القليل نسبيا.

ولكن لاحظ ما يجب أن يكون واضحا. في النموذج الذي وصفته القانون ينظم من خلال التنظيم المباشر- تنظيم الفرد من خلال التهديد بالعقاب threat of punishment. ولكن القانون ينظم بطرق أخرى أيضا. وهو ينظم، أي بشكل غير مباشر ومباشر. وينظم بشكل غير مباشر عندما ينظم هذه الطرائق الأخرى للقيد، بحيث تنظم بشكل مختلف. ويمكنه، أي تنظيم القواعد، وبالتالي فإن القواعد تنظم بطريقة مختلفة؛ يمكن أن ينظم السوق، بحيث ينظم السوق بشكل مختلف؛ ويمكن أن ينظم الهيكلة regulate architecture، بحيث تنظم الهيكلة بشكل مختلف. وفي كل حالة، يمكن للحكومة أن تُؤسس الهياكل الأخرى، بحيث تقيد الحكومة بنهايتها.

ذات التيه غير المباشر هو ممكن في العالم الافتراضي. ولكن هنا، أقترح، فإن التيه غير المباشر سوف يكون أكثر أهمية. وهنا فالحكومة تستطيع ليس فحسب التنظيم بشكل غير مباشر بأن يتقدّم ذلك نهاية خاصّة جوهريّة منها. والأهم من ذلك، يمكن للحكومة التنظيم لتغيير القابلية للتنظيم regulability. الحكومة، أي، يمكن تنظيم هياكل العالم الافتراضي، بحيث يصبح السلوك في العالم الافتراضي أكثر قابلية للتنظيم- وبالتأكيد، لإمكانية الهيكلة أن تكون أكثر قابلية للتنظيم من أي شيء عرفناه في تاريخ الحكومة الحديثة.
وهناك مثالان على ذلك: أحدهما مثال على تنظيم الحكومة لنهاية موضوعية معينة، والثاني، بعد الأول، مثال على تنظيم الحكومة لزيادة القدرة على التنظيم regulability.

الأول هو تنظيم التشفير regulation of encryption . كان اهتمام الحكومة بالتشفير هو استخدام التكنولوجيا في حماية الخصوصية protecting privacy- قدرتها على إخفاء محتوى الاتصالات content of communications عن أعين طرف ثالث متستر eavesdropping third party، سواء كان ذلك الطرف الثالث هو الحكومة، أو جار مزعج. على مدى جزء كبير من تاريخ هذه التكنولوجيا، قامت الحكومة الأميركية بتنظيم هذه التكنولوجيا بشكل كبير؛ وقد قامت الولايات المتحدة بـتنظيم هذه التكنولوجيا. لفترة من الوقت هددت بحظر استخدامها it threatened to ban its use، بل وقد حظرت باستمرار تصديرها (كما لو أن الأميركيين فقط يفهمون رياضيات النظام العالي higher order mathematics)؛ ولفترة من الزمن كان يأمل في إغراق السوق مع تكنولوجيا التشفير القياسية التي من شأنها أن تترك الباب الخلفي مفتوحة للحكومة للدخول.

وأحدث المقترحات هي الأكثر أهمية. حيث اقترح مكتب التحقيقات الفدرالي قانوناً يتطلب من المصنعين أن يضمنوا أن أي نظام تشفير قد بنى داخله إما قدرة رئيسية على التعافي، أو باباً خلفياً معادلاً، حتى يتمكن الوكلاء الحكوميون، إذا احتاجوا إلى ذلك، من الوصول إلى محتوى مثل هذه الاتصالات.

هذا هو تنظيم الحكومة للبرمجة، بشكل غير مباشر لتنظيم السلوك. إنه تنظيم غير مباشر بالمعنى الذي وصفته من قبل، ومن منظور دستوري- إنه تنظيم رائع. وليس رائع لأن غاياته جيدة؛ بل رائع لأن الدستور الأميركي، على الأقل، يقدم القليل جداً من السيطرة على التنظيم الحكومي من هذا القبيل. ولا يوفر الدستور الأميركي

سوى القليل من الحماية ضد تنظيم الحكومة للأعمال التجارية؛ ولا يوفر الدستور الأميركي سوى القليل من الحماية من تنظيم الحكومة للأعمال التجارية. ونظرا لمصالح الأعمال التجارية، من المرجح أن تكون هذه الأنظمة فعالة.

أما المثال الثاني فيتبعه من الأول. للاستخدام الثاني للتشفير هو تحديد الهوية identification— فضلا عن إخفاء ما يقول شخص ما، التشفير encryption، من خلال الشهادات الرقمية digital certificates، يمكن استخدامه لمصادقة من الذي بعض ذلك. مع القدرة على المصادقة authenticate على من هو الشخص، ويمكن للحكومة أن تعرف من أين يأتي شخص ما، أو كم هو عمره. وبهذه القدرة– من خلال التصديق على الشهادات- جوازات السفر على طريق المعلومات السريعة للغاية- يمكن للحكومات أن تنظم السلوك بسهولة أكبر بكثير على هذا الطريق السريع.

ومن شأنه أن يعيد إنشاء القدرة على السيطرة على السلوك - إعادة إنشاء القدرة على تنظيم.

لاحظ ما سوف تحققه اللائحتان. وبما أن الولايات المتحدة هي أكبر سوق لمنتجات الإنترنت، فلا يمكن لأي منتج أن يأمل في النجاح ما لم ينجح في الولايات المتحدة. وبالتالي فإن المعايير التي فرضت بنجاح في الولايات المتحدة تصبح معايير للعالم. وهذه المعايير على وجه الخصوص من شأنها أن تسهل أولاً التنظيم، وثانياً، ضمان أن الاتصالات على شبكة الإنترنت يمكن أن تقتحمها أية حكومة تتبع الإجراءات المبينة في مشروع القانون. ولكن المعايير التي يتعين على تلك الحكومة أن تفي بها ليست معايير الدستور الأميركي. فهي أية حكومة قياسية محلية تحدث أن يكون- سواء كانت تلك الحكومة هي حكومة الصين القارية، أو سويسرا.

والنتيجة هي أن حكومة الولايات المتحدة سوف تقوم بتصدير هيكلة تسهل السيطرة facilitates control، والسيطرة ليس فقط من قبل الحكومات الديمقراطية الأخرى، ولكن من قبل أية حكومة، مهما كانت قمعية repressive. وبهذا، فإن الولايات المتحدة سوف تنقل نفسها من رمز الحرية، إلى متجول في السيطرة. وبعد أن انتصرنا في الحرب الباردة، فإننا سوف ندفع بتقنيات أعدائنا في الحرب الباردة.

* * *

كيف يجب أن نستجيب؟ كيف ينبغي لكم- كأنصار سيادة مستقلون sovereigns independent عن نفوذ أي حكومة أجنبية- ونحن، كما يستجيب الدستوريون الليبراليون liberal constitutionalists؟ كيف ينبغي لنا أن نستجيب للتحركات التي تقوم بها قوة سياسية واقتصادية مهيمنة للتأثير على بنية الهيكل المهيمن للتنظيم عن طريق تعليمات البرمجة- الإنترنت؟

يجب أن يأتي أنصار السيادة لرؤية هذا: أن برمجة العالم الافتراضي هو في حد ذاته نوع من السيادة sovereign. وهو صاحب سيادة متنافسة competing sovereign. إن البرمجة في حد ذاتها قوة تفرض قواعدها الخاصة على الأشخاص الموجودين هناك، ولكن الناس الموجودين هناك هم أيضا الناس الموجودون هنا- مواطنو جمهورية الصين، ومواطنون من فرنسا، ومواطنون من كل أمة في العالم. وينظمها القانون، ومع ذلك فهي تخضع على نحو صحيح لتنظيم السيادة المحلية regulation of local sovereigns. وهكذا فإن البرمجة تتنافس مع السلطة التنظيمية للسيادة المحلية regulatory power of local sovereigns. وهي تتنافس مع الخيارات السياسية التي يتخذها المسؤولون المحليون political choices made by local sovereigns. وفي هذه المنافسة competition، كما تصبح الشبكة مكان مهيمن للأعمال والحياة

الاجتماعية، فإنه سيتم إزاحة تنظيمات المسؤولون المحلية. أنتم كدول ائن كانوا خائفين من النفوذ المتنافس للأمم ومع ذلك فإن أمة جديدة الآن تترابط في الهواتف الخاصة بك، ونفوذها على مواطنيكم آخذ في الازدياد.

أنت، كأنصار سيادة sovereigns، سوف تأتون للاعتراف بهذه المنافسة. ويجب أن تأتوا لتدركوا وتتساءلوا عن الدور الخاص الذي تلعبه الولايات المتحدة في هذه المسابقة. وبفضل توزيع الموارد التي تتحكم في هيكلة الشبكة، حيث تتمتع الولايات المتحدة بسلطة فريدة في التأثير على تطوير تلك الهيكلة. وهو كما تمت كتابة القانون الطبيعي law of nature, مع الولايات الأمريكيّة في المؤلفات في جانب اخر. هذه القوة تخلق مسؤولية مهمة للولايات المتحدة - ويجب أن تؤكدوا أنها تمارس سلطتها بمسؤولية.

والمشكلة التي يواجهها الدستوريون constitutionalists- أولئك المعنيون بالحفاظ على الحريات الاجتماعية والسياسية في هذا العالم الجديد - أكثر صعوبة.

وللعودة إلى القصة التي بدأت هذا الحديث- عالم جوازات السفر الداخلية. إحدى الطرق لفهم القصة التي قلتها اليوم عن العالم الافتراضي وهي تتماشى مع هذه القصة عن روسيا القيصرية. ولادة الشبكة كانت الثورة نفسها؛ كانت الحياة تحت شبكة Net 95 هي الحياة في روسيا بلشفية (الأجزاء الجيّدة على الأقلّ، حيث جوازات سفر داخليّة كانت قد أزلّيت)؛ فالشبكة كما هي عليه حالها أن تصبح روسيا ستالين، حيث سوف يطلب جوازات السفر الداخلية مرة أخرى.

الآن هناك غش cheat في تلك القصة- الغش بلاغي rhetorical cheat يميل إلى حجب حقيقة مهمة عن الحياة العالم الحقيقي. لأننا جميعا نعيش في عالم جوازات السفر الداخلية. في الولايات المتحدة، في أماكن كثيرة، لا يمكن للمرء أن يعيش بدون سيارة؛ لا يمكن للمرء أن يقود سيارة بدون ترخيص، الترخيص هو جواز سفر داخلي: فهو يقول من أنت، من أين أتيت، كم عمرك، ما إذا كنت قد أدانتك convicted مؤخراً بارتكاب جريمة؛ يربط هويتك بقاعدة بيانات من شأنها أن تكشف ما إذا كنت قد اعتقلت (سواء أدين أم لا) أو ما إذا كانت أي أوامر لاعتقالك في أية ولاية قضائية في البلاد معلقة. الرخصة هي جواز السفر الداخلي للدولة الأمريكية الحديثة. ولا شك أن قدرتها على السيطرة أو التحديد أفضل بكثير من روسيا القيصرية Tsar's Russia.

ولكن في الولايات المتحدة- على الأقل بالنسبة لأولئك الذين لا يبدو أن المهاجرين immigrants، أو أقلية غير مرغوب فيها- فان عبء هذه الجوازات طفيف. إن إرادة التنظيم والمراقبة والتتبع ليست قوية بما يكفي في الولايات المتحدة لدعم أي جهد منهجي لاستخدام جوازات السفر هذه للسيطرة على السلوك. والإرادة ليست قوية بما فيه الكفاية لأن تكلفة مثل هذه السيطرة كبيرة جدا. ولا توجد نقاط تفتيش checkpoints في كل زاوية؛ ولا يُطلب من المرء التسجيل عند الانتقال عبر المدينة؛ يمكن للمرء أن يمشي مجهول نسبيا معظم الوقت. إن تكنولوجيات السيطرة ممكنة، ولكنها في الأساس مكلفة للغاية. وهذه التكلفة هي، في جزء كبير منها، مصدر الحرية العظيمة. إن عدم الكفاءة في تكنولوجيات العالم الحقيقي التي تتحكم فيها هي التي تحقق حرية العالم حقيقية.

ولكن ماذا لو انخفضت تكلفة السيطرة بشكل كبير. ماذا لو ظهرت هيكلة تسمح بالمراقبة المستمرة؛ هيكلة تسهل التتبع المستمر للسلوك والحركة. ماذا لو ظهرت هيكلة من شأنها أن تجمع بلا تكلفة بيانات عن الأفراد، عن سلوكهم، حول من يريدون أن يصبحوا. وماذا لو كان يمكن للهيكلة أن تفعل ذلك بخفاء، دون التدخل في حياة يومية للأفراد على الإطلاق؟

هذه الهيكلة هي العالم الذي أصبحت عليه الشبكة. هذه هي صورة السيطرة التي تنمو فيها. كما هو الحال في العالم المادي/ الحقيقي، سيكون لدينا جوازات سفر في العالم الافتراضي. كما هو الحال في العالم الحقيقي، يمكن استخدام هذه الجوازات لتتبع سلوكنا. ولكن في العالم الافتراضي، على عكس العالم الحقيقي، هذا الرصد، هذا التتبع، هذا التحكم في السلوك، سيكون كل شيء أقل تكلفة بكثير. وهذا عنصر التحكم سوف يحدث في الخلفية، بشكل فعال وخفاء.
الآن لوصف هذا التغيير لا يعني ما إذا كان للخير أو للشر. والواقع أنني أقترح أن نعترف، باعتبارنا دستوريين، بوجود غموض جوهري fundamental ambiguity في أحكامنا السياسية الحالية بشأن الحرية والسيطرة liberty and control. أنا شعوبنا منقسمة في رد فعلهم على هذه الصورة لنظام السيطرة والكمال في وقت واحد، وهي صورة غير مرئية حتى الآن. كثيرون يقولون عن هذا النظام- انه رائع. كل ما هو أفضل لمحاصرة المذنبين، مع عبء ضئيل على الأبرياء. ولكن هناك الكثيرون أيضاً ممن يقولون عن هذا النظام- هو أمر مروع. وفي الوقت الذي أعلن في هنا مثلنا العليا في الحرية والتحرر من الحكم، كنا سننشئ نظاما للسيطرة أكثر فعالية بكثير من أي نظام في التاريخ من قبل.

لذا فإن الاستجابة لكل هذا ليست بالضرورة التخلي عن تكنولوجيات السيطرة technologies of control. الرد هو عدم الإصرار على أن شبكة Net95 بأن تكون الهيكلة الدائمة من الشبكة. الاستجابة بدلا من ذلك هي إيجاد وسيلة لترجمة ما هو بارز ومهم حول الحريات الحالية والديمقراطية الدستورية في هذا الهيكل من الشبكة. والنقطة هي أن يتم نقد قوة هذا السيادة- هذا السيادة الناشئة- وكما نحن ننتقد بشكل صحيح قوة أية سيادة.
ما هي هذه الحدود limits: بما أن الحكومة تسيطر على هيكل برمجة الشبكة أو تؤثر عليها، كحد أدنى، يجب أن نضمن أن الحكومة لا تحتكر تقنيات السيطرة هذه. يجب أن نؤكد أن أنواع الصكوك أن نبني في أية ديمقراطية دستورية constitutional democracy الية التوصل الى دمجها في التنظيم من قبل هذا الدستور- القانون. ويجب أن نضمن أن القيود التي تفرضها أية ديمقراطية دستورية- القيود المفروضة على الكفاءة التي تشكلها مشاريع قوانين الحقوق، ونظم الضوابط والموازين- تُدمج في التنظيم عن طريق البرمجة. هذه الحدود هي "الخلل bugs" في برمجة الديمقراطية الدستورية - وكما يقول جون بيري بارلو John Perry Barlow، يجب علينا أن نبني هذه الأخطاء في برمجة العالم الافتراضي. ويجب أن نبنيها حتى يتسنى لها، من خلال عدم كفاءتها، أن تعيد بعض أشكال الحماية التي عرفناها منذ زمن طويل.

ينظم القانون ثلاثة ارباع العالم الافتراضي، ولكن ليس فقط من خلال القانون. فبرمجة العالم الافتراضي هي واحدة من هذه القوانين. ويجب أن نرى كيف أن هذه البرمجة هي دولة ذات سيادة ناشئة emerging sovereign- منتشرة في كل مكان omnipresent، وملزمة omnipotent، ولطيفة gentle، وفعالة efficient، ومتنامية growing- وأنه يجب علينا أن نطور ضد هذه السيادة تلك الحدود التي وضعناها ضد سيادة العالم الحقيقي. وسوف يقول المسؤولون دائما - العالم الحقيقي وكذلك العالم الافتراضي- أن القيود، وعدم الكفاءة- الأخطاء bugs - ليست ضرورية.

ولكن الأمور تتحرك بسرعة كبيرة لمثل هذه الثقة. وخوفي ليس فقط أن هذا ضد السيادة، ونحن لم تتطور بعد لغة الحرية. ولا أننا لم يكن لدينا الوقت لتطوير مثل هذه اللغة. ولكن ما أخشاه هو أن نحافظ على الإرادة - إرادة المجتمعات الحرة على مدى القرنين الماضيين، في صياغة الدساتير لحماية الحرية، وعلى الرغم من أوجه الكفاءة.

الحوسبة الكمية (Quantum Computing)

إعداد:
المهندس بشير فرج برونوص
باحث في مجال تقنية المعلومات

Prepared by:
Eng. Bashir Faraj Brunoos
Researcher in Information Technology

الحوسبة الكمية: ثورة في عالم الحوسبة

مقدمة

تُعتبر الحوسبة الكمية (Quantum Computing) واحدة من أكثر الابتكارات إثارةً في مجال التكنولوجيا الحديثة. تستند هذه التقنية إلى مبادئ ميكانيكا الكم، وتعد بإحداث ثورة في كيفية معالجة المعلومات وحل المشكلات المعقدة. مع تقدم التكنولوجيا، أصبحت الحاجة إلى فهم الحوسبة الكمية وتأثيراتها المحتملة على مختلف المجالات، بما في ذلك العملات الرقمية مثل البيتكوين، أمرًا بالغ الأهمية. في هذا المقال، سنستعرض مفهوم الحوسبة الكمية، تطبيقاتها المختلفة، وتحدياتها، بالإضافة إلى تأثيرها المحتمل على العملات الرقمية.

ما هو الحوسبة الكمية؟

الحوسبة الكمية هو فرع من علوم الحاسوب يهدف إلى تطوير حواسيب تستخدم الكيوبيتات (qubits) بدلاً من البتات (bits) التقليدية. الكيوبيتات يمكن أن تكون في حالات متعددة في نفس الوقت (التراكب)، مما يمنح الحواسيب الكوانتية القدرة على معالجة المعلومات بشكل أسرع وأكثر كفاءة. هذه القدرة على التراكب والتشابك (entanglement) تعطي الحواسيب الكوانتية ميزة كبيرة في معالجة البيانات المعقدة.

الفرق بين الحوسبة التقليدية والحوسبة الكوانتية

في الحوسبة التقليدية، تعتمد العمليات على البتات، حيث يمكن لكل بت أن يكون في حالة واحدة فقط (0 أو 1) في أي وقت. في المقابل، تستخدم الحوسبة الكوانتية الكيوبيتات، التي يمكن أن توجد في حالات متعددة في نفس الوقت، مما يسمح بإجراء عمليات حسابية متوازية ومعقدة بشكل أسرع بكثير. هذا الاختلاف الجوهري في كيفية معالجة المعلومات هو ما يجعل الحوسبة الكمية مثيرًا للاهتمام.

تاريخ الحوسبة الكمية

البدايات

تعود جذور الحوسبة الكمية إلى أواخر الثمانينات، عندما بدأ العلماء في استكشاف فكرة استخدام مبادئ ميكانيكا الكم في الحوسبة. في عام 1981، قدم العالم ريتشارد فاينمان فكرة أن الحواسيب التقليدية قد لا تكون قادرة على محاكاة الأنظمة الكمومية بشكل فعال، مما أدى إلى اقتراح تطوير حواسيب تعتمد على مبادئ الكم.

تقدم الأبحاث

في السنوات التالية، تم تطوير العديد من الخوارزميات الكوانتية، مثل خوارزمية شور (Shor's algorithm) التي يمكن أن تحل مشاكل تحليل الأعداد الكبيرة بشكل أسرع من أي خوارزمية تقليدية، وخوارزمية غروGrover's algorithm) ver) التي تقدم تحسينات كبيرة في البحث في قواعد البيانات غير المرتبة. هذه الخوارزميات أظهرت الإمكانات الكبيرة للكوانتوم كومبيتنق في مجالات متعددة.

التطورات الحديثة

في العقد الأخير، شهدت أبحاث الحوسبة الكمية تقدمًا ملحوظًا، حيث تم تطوير حواسيب كوانتية قادرة على إجراء عمليات حسابية معقدة. في عام 2019، أعلنت شركة غوغل أنها حققت "تفوقًا كميًا" (quantum supremacy) من خلال إجراء عملية حسابية باستخدام حاسوب كوانتي في 200 ثانية، بينما كانت ستستغرق أكثر من 10,000 سنة باستخدام أقوى حاسوب تقليدي. هذه الإنجازات تعكس الإمكانيات الكبيرة التي يمكن أن تقدمها الحوسبة الكمية.

تطبيقات الحوسبة الكمية

1. الأمان السيبراني

تعد الحوسبة الكمية واعدة في مجال الأمان السيبراني، حيث يمكن أن تُستخدم لتطوير خوارزميات تشفير جديدة تكون أكثر أمانًا من الخوارزميات الحالية. تعتمد معظم أنظمة الأمان الحالية على خوارزميات تعتمد على صعوبة تحليل الأعداد الكبيرة، مثل خوارزمية RSA. ومع ذلك، يمكن أن تؤدي الحواسيب الكوانتية إلى اختراق هذه الخوارزميات بسهولة.

2. تشفير الكوانتوم

يمكن أن تُستخدم الحوسبة الكمية لتطوير تقنيات تشفير جديدة تعتمد على مبادئ الكم، مثل التشفير الكمي (quantum cryptography). يعتمد هذا النوع من التشفير على مبادئ ميكانيكا الكم لضمان أمان الاتصال، حيث يمكن اكتشاف أي محاولة للاعتراض.

3. الذكاء الاصطناعي

يمكن أن تُستخدم الحوسبة الكمية لتحسين تقنيات التعلم الآلي، حيث يمكنها معالجة كميات هائلة من البيانات بسرعة أكبر. هذا يمكن أن يعزز من قدرات الذكاء الاصطناعي في مجالات مثل الرؤية الحاسوبية ومعالجة اللغة الطبيعية. على سبيل المثال، يمكن استخدام الحواسيب الكوانتية لتحسين نماذج التعلم العميق، مما يؤدي إلى نتائج أكثر دقة وسرعة في التعلم.

4. الأدوية والبيولوجيا

تتيح الحوسبة الكمية محاكاة التفاعلات الكيميائية المعقدة، مما يمكن العلماء من تطوير أدوية جديدة بشكل أسرع وأكثر كفاءة. يمكن أن تسهم هذه التكنولوجيا في معالجة الأمراض المستعصية وتحسين الرعاية الصحية. على سبيل المثال، يمكن استخدام الحواسيب الكوانتية لمحاكاة تفاعلات الأدوية مع البروتينات، مما يساعد في تحديد الأدوية الأكثر فعالية.

5. تحليل البيانات

تُستخدم الحوسبة الكمية في تحليل كميات ضخمة من البيانات بسرعة تفوق الحواسيب التقليدية. هذا يمكن أن يكون مفيدًا في مجالات مثل المالية، حيث يمكن تحليل الاتجاهات السوقية بشكل أسرع. يمكن أن تساعد هذه القدرة في اتخاذ قرارات استثمارية أكثر دقة.

6. العملات الرقمية

تأثير الحوسبة الكمية على البيتكوين بينما تعتبر البيتكوين واحدة من أشهر العملات الرقمية، فإن تأثير الحوسبة الكمية يمتد إلى جميع العملات الرقمية. يمكن أن تؤدي الحوسبة الكوانتية إلى زيادة سرعة عمليات التعدين، مما قد يغير من طريقة تأكيد المعاملات. ومع ذلك، فإن الحوسبة الكوانتية قد تطرح تحديات أمنية خطيرة، حيث يمكن أن تُستخدم لاختراق البروتوكولات الأمنية الحالية، مما يتطلب تطوير خوارزميات جديدة مقاومة للهجمات الكوانتية.

7. تحسين الشبكات

تُستخدم الحوسبة الكمية لتحسين الشبكات، بما في ذلك الشبكات اللامركزية. يمكن أن تساعد هذه التكنولوجيا في تحسين كفاءة نقل البيانات وتقليل التأخير، مما يجعل الشبكات أكثر فعالية.

التحديات المستقبلية

1. الأمان

تظل مسألة الأمان إحدى أكبر التحديات التي تواجه الحوسبة الكمية. يجب على الباحثين تطوير خوارزميات جديدة تكون مقاومة للهجمات الكوانتية لضمان أمان المعلومات. يتطلب ذلك استثمارًا كبيرًا في البحث والتطوير، بالإضافة إلى التعاون بين مختلف القطاعات.

2. التكلفة

تطوير الحواسيب الكوانتية لا يزال مكلفًا، ويتطلب استثمارات كبيرة في البحث والتطوير. هذا قد يحد من انتشار هذه التكنولوجيا في المستقبل القريب. يجب على الحكومات والشركات الاستثمار في هذا المجال لضمان تحقيق الفوائد المحتملة.

3. الفهم العلمي

لا يزال هناك الكثير من الجوانب غير المفهومة في ميكانيكا الكم، مما يجعل البحث في هذا المجال معقدًا. يحتاج العلماء إلى فهم أعمق لهذه المبادئ لتطوير تطبيقات عملية فعالة. يتطلب ذلك تعاونًا دوليًا بين الباحثين والمؤسسات الأكاديمية.

4. التعليم والتدريب

مع تزايد الحاجة إلى مهارات الحوسبة الكمية، يجب على المؤسسات التعليمية تطوير برامج تعليمية لتدريب الجيل القادم من العلماء والمهندسين. يجب أن تشمل هذه البرامج مجالات متعددة، بما في ذلك علوم الحاسوب، والفيزياء، والهندسة.

الحوسبة الكمية في السياق العالمي

1. الدول الرائدة في الحوسبة الكمية

تسعى العديد من الدول إلى أن تكون رائدة في مجال الحوسبة الكمية. تتصدر الولايات المتحدة والصين هذا المجال، حيث تستثمر كلا الدولتين بشكل كبير في البحث والتطوير. تسعى الصين إلى تحقيق تقدم كبير في هذا المجال من خلال برامج حكومية تدعم الابتكار.

2. التعاون الدولي

تتطلب الأبحاث في الحوسبة الكمية تعاونًا دوليًا بين الدول والمؤسسات الأكاديمية. يمكن أن يؤدي التعاون إلى تبادل المعرفة والخبرات، مما يعزز من تقدم هذا المجال. يجب أن تشمل الشراكات بين الدول والمؤسسات الأكاديمية والقطاع الخاص.

3. التأثير على الاقتصاد العالمي

يمكن أن تؤدي الحوسبة الكمية إلى تغييرات كبيرة في الاقتصاد العالمي. من خلال تحسين الكفاءة في مختلف الصناعات، يمكن أن تساهم هذه التكنولوجيا في زيادة الإنتاجية والنمو الاقتصادي. ستؤدي التطبيقات المحتملة للكوانتوم كومبيتنق إلى خلق فرص عمل جديدة في مجالات التكنولوجيا والبحث.

التطبيقات المستقبلية للكوانتوم كومبيتنق

1. النقل الذكي

يمكن استخدام الحوسبة الكمية لتحسين نظم النقل الذكي، مما يؤدي إلى تقليل الازدحام وتحسين الكفاءة. يمكن أن تساعد هذه التكنولوجيا في تطوير أنظمة نقل تعتمد على البيانات الكبيرة وتحليلها.

2. الطاقة المتجددة

يمكن أن تُستخدم الحوسبة الكمية لتحسين تقنيات الطاقة المتجددة، مثل الطاقة الشمسية وطاقة الرياح. من خلال تحليل البيانات بشكل أسرع، يمكن تحسين كفاءة إنتاج الطاقة.

3. الأمن الغذائي

يمكن أن تُستخدم الحوسبة الكمية في تحسين الزراعة الذكية، مما يؤدي إلى زيادة الإنتاجية وتحسين الأمن الغذائي. يمكن أن تساعد هذه التكنولوجيا في تطوير تقنيات جديدة لتحليل التربة والمياه.

التحديات الأخلاقية والاجتماعية

1. تأثير الحوسبة الكمية على الخصوصية

مع تقدم الحوسبة الكمية، قد تزداد المخاوف بشأن الخصوصية. يمكن أن تؤدي القدرة على تحليل البيانات بسرعة إلى انتهاك الخصوصية الفردية. يجب أن تكون هناك قوانين وأنظمة واضحة لحماية الخصوصية.

2. الفجوة الرقمية

يمكن أن تؤدي الحوسبة الكمية إلى زيادة الفجوة الرقمية بين الدول المتقدمة والنامية. يجب أن تكون هناك جهود دولية لضمان وصول التكنولوجيا إلى جميع الدول، وتوفير التدريب والموارد اللازمة.

3. التأثير على سوق العمل

يمكن أن تؤدي الحوسبة الكمية إلى تغييرات كبيرة في سوق العمل. بينما ستخلق هذه التكنولوجيا فرص عمل جديدة، قد تؤدي أيضًا إلى فقدان الوظائف التقليدية. يجب أن تكون هناك برامج تدريبية لمساعدة العمال على التكيف مع التغيرات في سوق العمل.

مجالات البحث المستقبلية

- تطوير خوارزميات مقاومة للهجمات الكوانتية: يجب أن تركز الأبحاث على إنشاء بروتوكولات أمان جديدة تكون قادرة على حماية البيانات من التهديدات الكوانتية.

- تحليل تأثير الحوسبة الكمية على الشبكات اللامركزية: يجب دراسة كيفية تأثير الحوسبة الكمية على أداء الشبكات اللامركزية، مثل شبكات البلوكشين.

- استكشاف التطبيقات المحتملة في مجالات جديدة: يجب البحث في كيفية استخدام الحوسبة الكمية في مجالات مثل الزراعة الذكية والطاقة المتجددة.

إن فهم الحوسبة الكمية وتأثيرها المحتمل هو خطوة أساسية نحو مستقبل أكثر أمانًا وابتكارًا في عالم التكنولوجيا. يتطلب ذلك التعاون بين مختلف القطاعات، بما في ذلك الحكومة، والأكاديميا، والصناعة، لضمان تحقيق الفوائد الكاملة لهذه التكنولوجيا الرائدة.

الخاتمة

تُعتبر الحوسبة الكمية ثورة في عالم الحوسبة، ولها تأثيرات عميقة على مجموعة متنوعة من المجالات، بما في ذلك الأمان السيبراني، الذكاء الاصطناعي، والطب. بينما تعد العملات الرقمية مثل البيتكوين جزءًا من هذا المشهد المتغير، فإن التحديات المتعلقة بالأمان والتكلفة تبقى قائمة. من الضروري أن يتعاون الباحثون وصناع القرار لتطوير حلول مبتكرة تضمن أمان المعلومات في عصر الحوسبة الكوانتية.

مراجع

1. "Quantum Computation and Quantum Information"

- المؤلفون: مايكل نيلسن، إدواردو كيرش

- الناشر: Cambridge University Press

- تاريخ النشر: 2000 (الإصدار الثاني 2010)

- وصف: يعتبر هذا الكتاب مرجعًا أساسيًا في مجال الحوسبة الكوانتية ويغطي العديد من المواضيع الأساسية.

2. "Quantum Computing for Computer Scientists"

- المؤلفون: Noson S. Yanofsky, Mirco A. Mannucci

- الناشر: Cambridge University Press

- تاريخ النشر: 2008

- وصف: يقدم هذا الكتاب مقدمة شاملة حول الحوسبة الكمية بطريقة مفهومة لعلماء الحاسوب.

3. "Quantum Computing: A Gentle Introduction"

- المؤلفون: Eleanor Rieffel, Wolfgang Polak

- الناشر: MIT Press

- تاريخ النشر: 2011

- وصف: يقدم هذا الكتاب مقدمة سلسة للمفاهيم الأساسية في الحوسبة الكمية.

4. "The Quantum World: Quantum Physics for Everyone"

- المؤلف: Kenneth W. Ford

- الناشر: Harvard University Press

- تاريخ النشر: 2008

- وصف: يشرح هذا الكتاب مبادئ ميكانيكا الكم بطريقة مبسطة للجمهور العام.

5. "Quantum Computing: An Overview"

- المؤلف: Michael A. Nielsen

- الناشر: Springer

- تاريخ النشر: 2019

- وصف: يقدم هذا الكتاب لمحة شاملة عن الحوسبة الكوانتية وتطبيقاتها.

6. "Post-Quantum Cryptography"

- المحررون: Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen

- الناشر: Springer

- تاريخ النشر: 2009

- وصف: يتناول هذا الكتاب التحديات الأمنية التي تواجه التشفير التقليدي في عصر الحوسبة الكوانتية.

فقه الطرف الثالث

THE CASE FOR THE THIRD-PARTY DOCTRINE

البروفيسور اورين كير

Orin S. Kerr

THE CASE FOR THE THIRD-PARTY DOCTRINE

Orin S. Kerr

Michigan Law Review Vol. 107:561

Electronic copy available at: https://ssrn.com/abstract=1138128

Professor, George Washington University Law School. This Article benefited greatly from thoughtful comments during workshops at Seton Hall, Widener-Wilmington, and the GW/Berkeley Privacy Law Scholars Conference. Thanks in particular to Daniel Solove, Christopher Slobogin, David Feige, Stephen Henderson, and Christine Jolls.

تقدم هذه الدراسة دفاعا عن فقه الطرف الثالث في التعديل الرابع للدستور the Fourth Amendment's third-party doctrine، وهي القاعدة المثيرة للجدل controversial rule، حيث تفقد المعلومات حماية التعديل الرابع عندما يتم الكشف عنها عن علم لطرف ثالث. هاجم فقهاء التعديل الرابع مرارا وتكرارا القاعدة على أساس أنها غير مقنعة في ظاهرها وتمنح الحكومة الكثير من السلطة. يرد هذا المقال بأن النقاد قد أغفلوا فوائد القاعدة وبالغوا في نقاط ضعفها.

يخدم فقه الطرف الثالث وظيفتين حاسمتين:

أولا، يضمن المبدأ الحياد التكنولوجي technological neutrality للتعديل الرابع. وهو يصحح تأثير الاستبدال للأطراف الثالثة التي من شأنها أن تسمح للمجرمين الأذكياء savvy criminals باستبدال تصرف طرف ثالث خفي بفعل عام سابق.

ثانيا، يساعد الفقه على ضمان وضوح قواعد التعديل الرابع. إنه يطابق قواعد التعديل الرابع مع قواعد الموقع، مما يخلق الوضوح دون الحاجة إلى إطار معقد من القواعد الفريدة.

وأخيرا، فإن الانتقادين الأساسيين لفقه الطرف الثالث أضعف بكثير مما ادعى النقاد. إن مبدأ الطرف الثالث محرج لأسباب تتعلق بالشكل وليس بالوظيفة. إنها قاعدة موافقة متنكرة في شكل تطبيق لاختبار كاتس "التوقع المعقول للخصوصية reasonable expectation of privacy". الادعاءات بأن العقيدة تمنح الحكومة الكثير من السلطة تتجاهل بدائل حماية التعديل الرابع في استخدام الأطراف الثالثة. وتشمل هذه البدائل قانون الفخ، وامتيازات القانون العام، وفقه مسايا Massiah doctrine، والتعديل الأول، ولوائح الوكالة الداخلية internal agency regulations، وحقوق الأطراف الثالثة نفسها.

قائمة الفهرس

Table of Contents

2. فقه مبدأ مسايا

3. التعديل الاول

4. اللوائح الداخلية للوكالة

C. بدائل لحماية التعديل الرابع في قضايا سجلات الأعمال

1. الحماية التشريعية

2. امتيازات القانون العام/ السوابق

3. حقوق الاطراف الثالثة

خاتمة

مقدمة

Introduction

البشر/ الانسان Human beings هو حيوان اجتماعي social animals. فنحن نود أن نشارك. ونحب القيل والقال gossip. ونطلب المساعدة من الآخرين، ونقدم المساعدة في المقابل. في بعض الأحيان نشارك من خلال التحدث شخصيا. في بعض الأحيان نكتب خطابا أو نرسل رسالة عبر الحاسوب. وفي جميع هذه الحالات، يخلق الدافع البشري impulse للمشاركة فرصة مهمة للمحققين الجنائيين criminal investigators. عندما يشارك مرتكبوا الخطأ/ المخطئون wrongdoers مع الآخرين، فإنهم غالبا ما يكشفون أدلة على جرائمهم. قد يكشف زعيم عصابات فاسد mob boss عن السجلات لمحاسبه. قد يخبر رئيس الغوغاء شقيقه عن اعتداء. قد يكشف تاجر مخدرات عن خططه لمخبر سري. في جميع هذه الحالات، يأتي شخص آخر غير المجرم أو الشرطة- طرف ثالث- يحوز possess أدلة على الجريمة. غالبا ما يرغب المحققون في جمع الأدلة من هذه الأطراف الثالثة، حيث من المرجح أن يتعاونوا وأقل عرضة لإبلاغ المشتبه به بأن التحقيق يجري على قدم وساق investigation is afoot.

"ان فقه الطرف الثالث third-party doctrine" هي قاعدة التعديل الرابع التي تحكم جمع الأدلة من أطراف ثالثة في التحقيقات الجنائية[1]. فالقاعدة بسيطة: من خلال الكشف لطرف ثالث، يتخلى الموضوع عن جميع حقوقه في التعديل الرابع في المعلومات التي تم الكشف عنها. وفقا للمحكمة العليا:

لا يحظر التعديل الرابع الحصول على المعلومات التي يتم الكشف عنها لطرف ثالث ونقلها إلى السلطات الحكومية، حتى لو تم الكشف عن المعلومات على افتراض أنها لن تستخدم إلا لغرض محدود وأن الثقة الموضوعة في الطرف الثالث لن تتعرض للخيانة[2]. بمعنى آخر، لا يمكن لأي شخص أن يكون لديه توقع معقول للخصوصية reasonable expectation of privacy في المعلومات التي يتم الكشف عنها لطرف ثالث[3]. فالتعديل الرابع ببساطة لا ينطبق.

يعد فقه الطرف الثالث قاعدة التعديل الرابع التي يحب الفقهاء scholars كراهيتها/ أن يكرهوها. حيث إنه في قضية Lochner[4] لقانون التفتيش والضبط search and seizure law، والذي انتقد على نطاق واسع باعتباره مضللا للغاية profoundly is guided[5]. فالقرارات التي تطبق رؤية الفقه "تتصدر مخطط

[1] The "third-party doctrine" is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations. Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477, 528–29 (2006) (describing the third-party doctrine).

[2] United States v. Miller, 425 U.S. 435, 443 (1976). The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed. In other words, a person cannot have a reasonable expectation of privacy in information disclosed to a third party.3 The Fourth Amendment simply does not apply.

[3] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[4] Lochner v. New York, 198 U.S. 45 (1905).

[5] A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote. However, some of the major criticisms include Gerald G. Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy", 34 Vand. L. Rev. 1289, 1315 (1981); Lewis R. Katz, In Search of a Fourth Amendment for the Twenty-first Century, 65 Ind. L.J. 549, 564–66 (1990); Arnold H. Loewy, The Fourth Amendment as a Device for Protecting the Innocent, 81 Mich. L. Rev. 1229

حالات التعديل الرابع الأكثر انتقادا"[6]. ويؤكد (واين لافاف) Wayne LaFave في أطروحته المؤثرة أن قرارات المحكمة التي تطبقها "خاطئة تماما dead wrong"[7] و"تسخر من التعديل الرابع make a mockery of the Fourth Amendment"[8]. فقد كان منطوق الحكم verdict بين المعلقين commentators متكررا frequent وبالإجماع unanimous على ما يبدو: ذلك ان قاعدة فقه الطرف الثالث ليست خاطئة فحسب[9]، ولكنها خاطئة بشكل فظيع[10]. وحتى أن العديد من قضاة محاكم الولاية وافقوا على ذلك. وقد رفضت أكثر من اثنتي عشرة محكمة عليا في الولايات هذا المبدأ بموجب أحكام موازية من دساتير ولاياتها[11].

ومن اللافت للنظر أنه حتى المحكمة العليا الأمريكية لم تقدم أبدا حجة واضحة لصالحها. وقد طبق العديد من فتاوى المحكمة العليا هذا المبدأ. قليلون دافعوا عنه. وكان أقرب ما توصلت إليه المحكمة لتبرير هذا المبدأ هو تأكيدها العرضي على أن الأشخاص الذين يكشفون عن الاتصالات لطرف ثالث "يتحملون المخاطرة assume the risk" بأن معلوماتهم ستنتهي في أيدي الشرطة[12]. ولكن افتراض الخطر هو نتيجة وليس مبررا But assumption of risk is a result rather than a rationale: يجب على الشخص أن

(1983) (arguing that the third-party doctrine cases are incorrect because they focus on the rights of the guilty rather than the rights of the innocent); Scott E. Sundby, "Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?, 94 Colum. L. Rev. 1751, 1757–58 (1994).
Recent criticisms of the doctrine include Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 151–64 (2007); Susan W. Brenner & Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data, 14 J.L. & Pol'y 211 (2006) (arguing that the major third-party doctrine cases were wrongly decided on several grounds); Susan Freiwald, First Principles of Communications Privacy, 2007 Stan. Tech. L. Rev. 3; Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 Pepp. L. Rev. 975 (2007); Matthew D. Lawless, The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection, 2007 UCLA J.L. & Tech. 1, 3–4 (advocating a "retooling" of the third-party doctrine for internet searches); Andrew J. DeFilippis, Note, Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence, 115 Yale L.J. 1086, 1092 (2006) (arguing that the Supreme Court should overrule the third-party doctrine).

[6] Clark D. Cunningham, A Linguistic Analysis of the Meanings of 'Search' in the Fourth Amendment: A Search for Common Sense, 73 Iowa L. Rev. 541, 580 (1988). Decisions applying the doctrine "top the chart of the most-criticized fourth amendment cases.".

[7] Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 2.7(c), at 747 (4th ed. 2004).

[8] Id. § 2.7(b), at 736 ("Such a crabbed interpretation of the Katz test makes a mockery of the Fourth Amendment.").

[9] See sources cited supra note 5.

[10] See, e.g., 1 LaFave, supra note 7, § 2.7(c), at 747 ("The result reached in Miller is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in Katz."); Daniel J. Solove, Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference, 74 Fordham L. Rev. 747, 753 (2005) ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

[11] For a list of states that have rejected the doctrine, in whole or in part, see Stephen E. Henderson, Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Amalog's To Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373 (2006).

[12] Smith v. Maryland, 442 U.S. 735, 744 (1979) ("Because the depositor [in Miller] 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.").

يتحمل الخطر فقط عندما لا يحميه الدستور. وبالضبط لماذا لا يحمي الدستور المعلومات التي يتم الكشف عنها لأطراف ثالثة تركت دون تفسير unexplained.

تقدم هذه الدراسة دفاعا عن قاعدة فقه الطرف الثالث، وخاصة تطبيقاتها الأكثر إثارة للجدل most controversial applications. حيث تجادل بأن هذه القاعدة تخدم دورين غاب عنهما النقاد. الغرض الأول والأهم هو الحفاظ على الحياد التكنولوجي لقواعد التعديل الرابع. وان استخدام الأطراف الثالثة له تأثير متغير substitution effect:

فهي تأخذ أجزاء علنية من الجرائم وتخفيها عن المراقبة العامة public observation. وبدون فقه الطرف الثالث، يمكن للمخطئين الدهاة savvy wrongdoers استخدام خدمات الطرف الثالث بطريقة تكتيكية لإخفاء كامل جرائمهم في إطار الحماية التي يفرضها التعديل الرابع.

والنتيجة هنا من شأنها أن تسمح للتكنولوجيا بالإخلال بالتوازن التقليدي للتعديل الرابع بين الخصوصية privacy والأمن security، مما يضعف الأهداف الرادعة والعقابية للعقوبة الجنائية. حيث يمنع فقه الطرف الثالث هذا الالتفاف حول التوازن التقليدي للتعديل الرابع. وإنه يساعد على ضمان أن قواعد التعديل الرابع التي تنطبق على الجرائم المرتكبة باستخدام أطراف ثالثة تعادل تقريبا القواعد التي تنطبق على الجرائم المرتكبة بدونها.

والدور الثاني لهذا الفقه هو توفير الوضوح المسبق. بموجب مبدأ فقه الطرف الثالث، حيث تتطابق حماية التعديل الرابع للمعلومات مع حماية التعديل الرابع للبيئة التي يتم تخزينها فيها. نتيجة لذلك، يتم تحديد قواعد التعديل الرابع من خلال الموقع المعروف للمعلومات بدلا من تاريخها غير المعروف. وفي غياب مبدأ فقه الطرف الثالث، ستواجه المحاكم التحدي الصعب المتمثل في إنشاء نظام واضح لحماية التعديل الرابع لمعلومات الطرف الثالث. وعلى الرغم من أن مثل هذه التحديات ليست مستعصية على الحل، إلا أن وضوح عقيدة الطرف الثالث يوفر حجة مهمة لصالحها.

ان فقه الطرف الثالث ليس حلا سحريا no panacea، وبالطبع. قدم النقاد حجتين مهمتين ضدها، إحداهما عقائدية doctrinal والأخرى وظيفية functional[13]. والحجة العقائدية هي أن القضاة لا يفهمون مصالح الخصوصية على المحك في معلومات الطرف الثالث. بالنسبة لهؤلاء النقاد، فإن تأكيد القضاة على أن الكشف يجعل تلقائيا توقع الخصوصية "expectation of privacy" غير معقول "unreasonable" هو ببساطة غير صحيح[14]. والحجة الثانية وظيفية: فهي تؤكد أن المبدأ مضلل لأنه يمنح الحكومات سلطة اتخاذ خطوات أكثر تدخلا invasive steps دون إشراف دستوري مما يتفق مع مجتمع حر ومفتوح. وعلى وجه الخصوص، يمنح مبدأ فقه الطرف الثالث المسؤولين الحكوميين الكثير من السلطة لمضايقة harass الأفراد بسوء نية[15].

وتوضح هذه الدراسة أنه في حين أن كلا الانتقادين لهما بعض الجاذبية، إلا أن كلاهما يبالغ إلى حد كبير في القضية ويتجاهل الحجج المضادة المهمة important counterarguments. والتأكيدات بأن القضاة لا يفهمون الخصوصية هي اعتراضات حول الشكل form أكثر من الجوهر substance. على الرغم من أن مبدأ فقه الطرف الثالث قد تم تأطيره من حيث اختبار "التوقع المعقول للخصوصية"، إلا أنه من الأفضل

[13] See infra Section I.B.
[14] See infra Section I.B.1.
[15] See infra Section I.B.2.

فهمه على أنه مبدأ فقه الارادة consent doctrine. حيث ان الكشف لأطراف ثالثة يلغي الحماية لأنه يعني الارادة. اذ عندما يفهم على أنه مجموعة فرعية من قانون الارادة consent law بدلا من تطبيق التوقع المعقول لاختبار الخصوصية، فإن فقه الطرف الثالث يتناسب بشكل طبيعي مع بقية نصوص التعديل الرابع.

وأخيرا، تتجاهل الحجج الوظيفية functional arguments سلطة الحكومة لبدائل النظام القانوني لحماية التعديل الرابع. التعديل الرابع ليس اللعبة الوحيدة المتوافرة. تم تصميم امتيازات القانون العام/ السوابق Common law privileges وقانون الفخ entrapment law[16] وفقه ماسياه Massiah doctrine ومبدأ التعديل الأول وحماية الخصوصية القانونية خصيصا تتواجد لمعالجة المخاوف من مضايقات الشرطة في استخدامها لأطراف ثالثة[17]. هذه المبادئ القانونية غير الدستورية في الغالب تنظم جوانب محددة من ممارسات الطرف الثالث لردع انتهاكات الشرطة deter police abuses، مما يجبر الشرطة عموما على استخدام أطراف ثالثة بحسن نية أو بطريقة معقولة. لقد تجاهل النقاد هذه البدائل، ونتيجة لذلك مالوا إلى رؤية الاختيار بين حماية التعديل الرابع أو عدم الحماية على الإطلاق. ثم إن فهم كيفية استبدال العقائد الأخرى بحماية التعديل الرابع يكشف أن هذا الفهم غير صحيح.

الهدف من هذه الدراسة هو استبدال النظرة الجزئية partial view لفقه الطرف الثالث الموجودة في المنح الدراسية الحالية بحساب أكثر ثراء وتوازنا لتكاليفها وفوائدها. يأتي الموضوع في الوقت المناسب: فالتقدم التكنولوجي يضع المزيد والمزيد من الاتصالات في أيدي أطراف ثالثة[18]، وقد أدت الأهمية المتزايدة للتكنولوجيات الجديدة مثل الإنترنت إلى تجديد الهجمات على عقيدة الطرف الثالث[19]. وبالنظر إلى الموجة الأخيرة من الانتقادات، هناك حاجة إلى فهم أكثر اكتمالا لتقدير أفضل لكيفية تطبيق التعديل الرابع في حالة التقنيات القديمة والجديدة. فلا أتوقع أن تقنع الحجج المقدمة في هذه الدراسة كل ناقد بتغيير مواقفه. وبما يمكن أن يختلف الأشخاص العقلاء حول ما إذا كان المبدأ مناسبا في حالات معينة. في الوقت نفسه، آمل أن تظهر الدراسة حجة إيجابية قوية للفقه في كثير من الحالات وحجة معقولة على الأقل في حالات أخرى.

وتنقسم هذه الدراسة إلى أربعة أجزاء. يقدم الجزء الأول بإيجاز قانون فقه الطرف الثالث law of the third-party doctrine والانتقادات القاسية له. يجادل الجزء الثاني بأن فقه الطرف الثالث تضمن الحياد التكنولوجي للتعديل الرابع من خلال منع الاستخدام الانتهازي لأطراف ثالثة للتحايل على التوازن الأساسي لقواعد التعديل الرابع.

ويؤكد الجزء الثالث أن المبدأ ضروري لتوفير الوضوح المسبق. ويتطلب علاج قمع التعديل الرابع قواعد واضحة تحكم متى يحدث بحث التعديل الرابع، ويخلق مبدأ الطرف الثالث هذا اليقين المطلوب. ويرد الجزء الرابع على الانتقادين الأساسيين لمبدأ الطرف الثالث، وهما أن العقيدة غير مقنعة من الناحية العقائدية وأنها

---

[16] **Entrapment is an affirmative legal defense.** In the most basic sense, it occurs when a government official, such as a police officer, uses threats, fraud, or harassment to induce or coerce someone to commit a crime they wouldn't ordinarily commit. Defendants who can prove with a preponderance of the evidence that entrapment has occurred will likely be acquitted of the charges for which they are being tried.
SEE: https://www.newjerseycriminallawattorney.com/criminal-process/what-does-entrapment-mean-in-a-legal-case/

[17] All of these doctrines are discussed infra Section IV.B.

[18] See Solove, supra note 1, at 528–29.

[19] See, e.g., sources cited supra note 5.

تعطي الشرطة سلطة أكثر مما ينبغي. وتجادل بأن الادعاء الأول هو إلى حد كبير مسألة شكلية وأن الأخير تتناوله قواعد قانونية تتجاوز التعديل الرابع.

I. مقدمة إلى فقه الطرف الثالث

I. Introduction to the Third-Party Doctrine

يشرح هذا الجزء مبدأ فقه الطرف الثالث ويلخص النوعين الأساسيين من الحالات: تلك التي تنطوي على عملاء سريين secret agents مثل المخبرين السريين undercover informants، وتلك التي تنطوي على سجلات حسابات account records طرف ثالث. يقدم هذا الجزء أيضا الانتقادين الأساسيين لعقيدة الطرف الثالث. النقد الأول ذو طبيعة فقهية doctrinal in nature. وتؤكد أنه من الخطأ ببساطة القول إن كشف exposure الطرف الثالث يجعل توقع الخصوصية "غير معقول"[20]. والنقد الثاني وظيفي functional. ويدعي أن مبدأ فقه الطرف الثالث يمنح الحكومة الكثير من السلطة على الأفراد[21].

A. القضايا

1. العملاء السريون 1952- 1971

A. The Cases

1. Secret Agents, 1952–1971

وعلى الرغم من أن العديد من القضايا الأولى للمحكمة العليا في قانون الإجراءات الجنائية law of criminal procedures تضمنت استخدام عملاء سريين undercover agents ومخبرين سريين confidential informants[22]. او - ما يسمى بـ.. "العملاء السريين "secret agents"[23]- فلم يصل تحدي التعديل الرابع لمثل هؤلاء العملاء السريين إلى المحكمة حتى قضية لي ضد الولايات المتحدة[24]. حيث باع لي الأفيون من متجر الغسيل الخاص به وأدلى ذات يوم بتصريحات تجرم incriminating صديقه (بوي) Poy. حيث اتضح أن (بوي) كان مخبرا سريا يرتدي سلك ميكروفون، وتم استخدام تسجيل تصريحاته ضده في المحاكمة. وجادل لي بأن سلوك الحكومة ينتهك التعديل الرابع لأنه كان يعادل وضع ميكروفون bug سرا داخل المتجر.

---

[20] See infra Section II.B.1.
[21] See infra Section II.B.2.
[22] For example, in Gouled v. United States, 255 U.S. 298 (1921), a business acquaintance of a criminal suspect pretended to pay a social visit at the suspect's office when he in fact was intending to search the office for evidence. Eleven years later, in Sorrells v. United States, 287 U.S. 435 (1932), an undercover prohibition agent looking for alcohol gained entrance to a suspect's home by posing as a tourist. Although these cases involved secret agents, they did not specifically raise Fourth Amendment challenges to secret agents' use.
[23] See, e.g., Yale Kamisar et al., Modern Criminal Procedure 465 (12th ed. 2008).
[24] Lee v. United States. 343 U.S. 747 (1952).

ولم توافق المحكمة العليا على ذلك. وفقا للقاضي جاكسون Justice Jackson، كان لي ببساطة "يتحدث بسرية وطائشة مع شخص يثق به was talking confidentially and indiscreetly with one he trusted"[25]. وحقيقة أن بوي كان يرتدي سلكا لم يكن ذا صلة، لأن التسجيل كان "بالتواطؤ مع أحد الطرفين with the connivance of one of the parties"[26] للمحادثة (أي بوي). اقترح القاضي جاكسون أن فكرة رؤية هذه الحقائق على أنها إشكالية بموجب التعديل الرابع كانت سخيفة للغاية: "ستكون خدمة مشكوك dubious service فيها للحريات الحقيقية التي يحميها التعديل الرابع لجعلهم رفقاء في الفراش مع حريات زائفة مرتجلة من خلال تشبيهات بعيدة المنال ... [27].

توصلت المحكمة إلى نفس النتيجة بعد عقد من الزمان في قضية لوبيز ضد الولايات المتحدة[28].27 حاول لوبيز رشوة عميل مصلحة الضرائب الذي كان يرتدي سلكا، وتم قبول كل من التسجيل وشهادة الوكيل ضد لوبيز في المحاكمة. نقلا عن On Lee، رفض القاضي (هارلان) Justice Harlan بسهولة ادعاء لوبيز بأن حقوقه في التعديل الرابع قد انتهكت: "كان لوبيز يعلم جيدا أن تصريحاته يمكن استخدامها ضده من قبل وكيل مصلحة الضرائب إذا رغب في ذلك[29]، "وجهاز التسجيل السلكي" تم استخدامه فقط للحصول على أكثر الأدلة موثوقية الممكنة لمحادثة كان فيها وكيل الحكومة مشاركا والتي كان لهذا الوكيل الحق الكامل في الكشف عنها disclose"[30].

تبع لوبيز بسرعة لويس ضد الولايات المتحدة Lewis v. United States [31] وهوفا ضد الولايات المتحدة Hoffa v. United States,[32] وصدر في نفس اليوم من عام 1966. في لويس، دعا المتهم عميلا سريا إلى منزله لبيعه الماريجوانا. وفي هوفا Hoffa، أسر رئيس Teamsters جيمي هوفا Jimmy Hoffa بزميله بارتين Partin، الذي تبين أنه يعمل سرا لصالح الشرطة.

في كلتا الحالتين، أدلى العملاء السريون في وقت لاحق بشهاداتهم حول ما رأوه وسمعوه. بالاعتماد على لوبيز وعلى لي، وخلصت المحكمة إلى أن أيا من استخدام العملاء السريين لم ينتهك التعديل الرابع. في حين أن هوفا "كان يعتمد على ثقته في غير محلها بأن بارتين لن يكشف عن مخالفاته"، فإن التعديل الرابع لا يحمي "اعتقاد مرتكب الخطأ في غير محله بأن الشخص الذي يعهد إليه طواعية بخطئه لن يكشف عنها"[33]. ولا يمكن أن يكون استخدام ضابط سري في لويس غير دستوري لأن مثل هذه القاعدة ستعرقل بشدة التحقيقات السرية:

فإذا اعتبرنا خداع deceptions العميل في هذه الحالة محظورا دستوريا، فسوف نقترب من قاعدة مفادها أن استخدام العملاء السريين بأي شكل من الأشكال غير دستوري في حد ذاته. ومن شأن هذه القاعدة، على

[25] Id. at 753.
[26] Id
[27] 373 U.S. 427 (1963).
[28] Lopez v. United States., Id. at 438.
[29] d. at 439.
[30] 385 U.S. 206 (1966).
[31] Lewis v. United States, 385 U.S. 206 (1966).
[32] Hoffa v. United States, 385 U.S. 293 (1966).
[33] the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.", Id. at 302.

سبيل المثال، أن تعوق الحكومة بشدة تحديد الأنشطة الإجرامية المنظمة التي تتسم بالتعامل السري مع الضحايا الذين لا يستطيعون الاحتجاج أو لا يحتجون[34].

آخر قضايا العملاء السريين، الولايات المتحدة ضد وايت United States v. White. أكد وايت[35]، أن عقيدة الطرف الثالث نجت من التحول الرسمي إلى التوقع المعقول لاختبار الخصوصية الذي تم التعبير عنه لأول مرة في موافقة القاضي هارلان في كاتز ضد الولايات المتحدة[36].

كانت حقائق وايت متطابقة تقريبا مع حقائق لوبيز: تحدث وايت عن جرائمه إلى مخبر سري كان يرتدي سلكا، واستخدمت تسجيلات المحادثات ضده في المحاكمة[37]. خلص رأي التعددية للقاضي في قضية وايت إلى أن هوفا ولوبيز وأون لي قد نجوا مما تقرر في قضية كاتز Katz[38]. ولم يزعج كاتز هذا الخط من القضايا لأنه "لم يتضمن أي كشف للحكومة من قبل طرف في المحادثات مع المتهم"[39]. وبلغة وايت، لم يكن توقع عدم مشاركة شخص ما لمعلومات خاصة مع الشرطة مبررا دستوريا:

لا مفر من أن الشخص الذي يفكر في أنشطة غير قانونية يجب أن يدرك ويخاطر بأن رفاقه قد يبلغون الشرطة. إذا كان يشك بما فيه الكفاية في مصداقيتهم، فمن المحتمل جدا أن تنتهي الجمعية أو لا تتحقق أبدا. ولكن إذا لم تكن لديه شكوك، أو هدأها، أو خاطر بما لديه من شك، فإن الخطر هو لديه[40].

بالضبط لماذا كان هذا الاستنتاج "لا مفر منه inescapable" - ولماذا "الخطر له the risk is his" - ترك دون تفسير.

2. السجلات التجارية، 1973-1980

2. Business Records, 1973–1980

حدثت الجولة الثانية من قضايا فقه الطرف الثالث من عام 1973 إلى عام 1980، وشملت جميعها أنواعا مختلفة من السجلات التجارية. في جميع القضايا، رأت المحكمة أن نقل السجلات التجارية إلى أطراف ثالثة تخلى عن حماية التعديل الرابع. وفي قضية Couch v. United States، أعطى Couch[41] مستندات ضريبية لمحاسبه، وأصدرت الحكومة استدعاء من مصلحة الضرائب يأمر المحاسب بتسليم المستندات المتعلقة بالإقرارات الضريبية لـ.. Couch [42] في 42 عاما [43]، قدمت الحكومة مذكرات استدعاء على البنوك التي استخدمها المتهم ميلر للحصول على جميع السجلات المتعلقة بحساباته. في قضية Payner [44] سرق

[34] 401 U.S. 745 (1971).
[35] United States v. White, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[36] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[37] White, 401 U.S. at 746–47.
[38] Id. at 749–50.
[39] Id. at 749. Because Justice Black's concurring opinion adopted a far broader rationale, Justice White's plurality opinion expresses the holding of the Court.
[40] Id. at 752.
[41] Couch v. United States, 409 U.S. 322 (1973).
[42] Id. at 324–25.
[43] United States v. Miller, 425 U.S. 435 (1976).
[44] United States v. Payner. 447 U.S. 727 (1980).

43 محققا حقيبة يملكها نائب رئيس بنك في جزر البهاما ثم نسخوا محتويات الحقيبة قبل إعادتها. كشفت المحتويات أن باينر احتفظ بحساب في البنك، وهذا ساعد الحكومة على إظهار أن باينر قد زور إقراراته الضريبية[45].

وفي جميع الحالات الثلاث، تحرك المتهم لقمع السجلات المالية بموجب التعديل الرابع. وفي جميع القضايا الثلاث، رفضت المحكمة الادعاءات بموجب مبدأ الطرف الثالث في آراء القاضي (باول). في Couch، خلص القاضي (باول) إلى أنه "لا يمكن أن يكون هناك توقع كبير للخصوصية حيث يتم تسليم السجلات إلى محاسب"[46].

من خلال تسليم المعلومات إلى محاسبه، أعطى Couch محاسبه سلطة تحديد المعلومات التي سيتم الكشف عنها بشكل أكبر في إقرارات ضريبة الدخل الخاصة بـ.. Couch [47] . وفي ميلر Miller، استخدم القاضي (باول) Powell حجتين مختلفتين. أولا، لم تكن السجلات المصرفية رسائل خاصة أو شخصية للمدعى عليه، بل كانت مستندات مالية يمكن استخدامها في سياق العمل العادي[48]. ثانيا، نقل المتهم المعلومات طواعية إلى طرف ثالث تماما مثل وايت وهوفا ولوبيز. "من خلال الكشف عن شؤونه لآخر"، افترض المتهم خطر "نقل المعلومات من قبل ذلك الشخص إلى الحكومة"[49]. وفي باينر، وجد القاضي (باول) أن القضية لا يمكن تمييزها عن ميلر[50].

وأخيرا، طبقت المحكمة مبدأ الطرف الثالث في قضية سميث ضد ماريلاند[51]، وهي قضية تتعلق باجهزة رقابة تسمى سجلات القلم pen registers. كان سجل القلم عبارة عن جهاز مثبت في شركة الهاتف لتسجيل الأرقام التي تم الاتصال بها من هاتف معين. وفي قضية سميث، طلب المحققون من شركة الهاتف تثبيت سجل قلم على هاتف منزل رجل يشتبه في قيامه بسرقة امرأة ثم مضايقتها من خلال إجراء مكالمات هاتفية مجهولة.

ولقد أكد جهاز سجل القلم أن المكالمات كانت صادرة من منزل الرجل، وأن المعلومات استخدمت للمساعدة في الحصول على أمر بتفتيش منزله[52].

ورأت المحكمة العليا أن استخدام جهاز سجل القلم ليس "بحثا" لأنه مشمول بمبدأ الطرف الثالث: "عندما استخدم صاحب الالتماس هاتفه، نقل طوعا معلومات رقمية إلى شركة الهاتف و"عرض" تلك المعلومات على معداتها في سياق العمل المعتاد. وبذلك، افترض مقدم الالتماس المخاطرة بأن تكشف الشركة للشرطة

---

[45] Id. at 728–30.
[46] "there can be little expectation of privacy where records are handed to an accountant". Couch, 409 U.S. at 335.
[47] See id. ("What information is not disclosed is largely in the accountant's discretion . . . . Indeed, the accountant himself risks criminal prosecution if he willfully assists in the preparation of a false return. His own need for self-protection would often require the right to disclose the information given him." (citation omitted)).
[48] Miller, 425 U.S. at 442.
[49] Id. at 443.
[50] Payner, 447 U.S. at 732 ("United States v. Miller established that a depositor has no expectation of privacy and thus no protectable Fourth Amendment interest in copies of checks and deposit slips retained by his bank. Nothing in the record supports a contrary conclusion in this case." (citations omitted) (internal quotation marks omitted)).
[51] Smith v. Maryland, 442 U.S. 735 (1979).
[52] Id. at 737.

عن الأرقام التي اتصل بها"[53]. وفقا للقاضي (بلاكمون)، الذي كتب نيابة عن الأغلبية، " معدات التبديل التي عالجت هذه الأرقام كانت مجرد نظير حديث للمشغل الذي أكمل شخصيا في يوم سابق مكالمات المشترك"[54]. وتم تطبيق مبدأ الطرف الثالث على الرغم من أن "شركة الهاتف قررت الأتمتة decided to automate"[55].

B. الانتقادات الشائعة لفقه الطرف الثالث

B. Common Criticisms of the Third-Party Doctrine

تنبع الانتقادات الموجهة إلى فقه الطرف الثالث من حجتين أساسيتين، واحدة فقهية doctrinal والأخرى وظيفية functional. تم تطوير كلتا الحجتين لأول مرة في معارضين من قضايا عقيدة الطرف الثالث المهمة، وأبرزها معارضة القاضي (هارلان) Justice Harlan في White [56] ومعارضة القاضي مارشال Justice Marshall في قضية سميث Smith [57]. وفي العقود التي تلت هذه الآراء، رددت مجموعة كبيرة من المنح الدراسية وتوسعت في ادعاءاتهم الأساسية.

1. النقد الفقهي

1. The Doctrinal Critique

ان أول انتقاد مهم لمبدأ الطرف الثالث هو أنه لا يطبق بدقة التوقع المعقول لاختبار الخصوصية. وفقا للنقاد، يتوقع الأفراد عادة الخصوصية في سجلاتهم المصرفية وسجلات الهاتف وسجلات الطرف الثالث الأخرى[58]. ومثل هذه التوقعات للخصوصية شائعة ومعقولة، والقضاة الذين لا يستطيعون رؤية ذلك هم ببساطة بعيدون عن المجتمع ويسيئون تطبيق التعديل الرابع. ومن هذا المنظور، "يتحدى الواقع defies reality"[59].فالقول بأن الشخص يسلم المعلومات "طواعية voluntarily" إلى أطراف ثالثة مثل البنوك أو شركات الهاتف[60]. كما قال القاضي مارشال Justice Marshall في معارضة قضية سميث، "من العبث الحديث عن" افتراض assuming" المخاطر في السياقات التي، من الناحية العملية، ليس لدى الأفراد بديل واقعي"[61].

---

[53] Id. at 744.
[54] Id.
[55] Id. at 745.
[56] United States v. White, 401 U.S. 745, 768–95 (1971) (Harlan, J., dissenting)
[57] Smith, 442 U.S. at 748–52 (Marshall, J., dissenting).
[58] See, e.g., Ashdown, supra note 5, at 1315 (“[T]elephone patrons undoubtedly would be shocked to learn that records of their calls either were available for third parties or were being distributed outside the telephone system.”); Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society”, 42 Duke L.J. 727, 732 (1993) (arguing that some Supreme Court cases “do not reflect societal understandings” of when an expectation of privacy is “reasonable,” and that “some of the Court’s conclusions [about what expectations of privacy are reasonable] may be well off the mark”).
[59] See Slobogin & Schumacher, supra note 57, at 732.
[60] Christopher Slobogin, Subpoenas and Privacy, 54 DePaul L. Rev. 805, 829 (2005).
[61] See also Ashdown, supra note 5, at 1315.

النتيجة الطبيعية لهذا الادعاء هي أن القضاة الذين يدعمون مبدأ الطرف الثالث قد أساءوا فهم مفهوم الخصوصية. يتصور القضاة الخصوصية كمفتاح تشغيل وإيقاف، يساوي الكشف عن واحد مع الكشف للجميع، ونتيجة لذلك يفتقدون العديد من ظلال اللون الرمادي[62]. كما قال القاضي مارشال Justice Marshall في قضية سميث Smith، ان الخصوصية "privacy" ليست سلعة منفصلة discrete commodity، تحوزها بشكل مطلق possessed absolutely أو لا تحوزها على الإطلاق.

أولئك الذين يكشفون عن حقائق معينة لبنك أو شركة هاتف لغرض تجاري محدود لا يحتاجون إلى افتراض أن هذه المعلومات سيتم الكشف عنها لأشخاص آخرين لأغراض أخرى"[63]. مرددا صدى القاضي مارشال Echoing Justice Marshall، وحيث يجادل (دانيال سولوف) Daniel Solove بأن فقه الطرف الثالث يستند إلى "مفهوم غير صحيح للخصوصية incorrect conception of privacy"، وهو مفهوم للخصوصية على أنها سرية تامة total secrecy [64]. وعلى نفس المنوال، يجادل (ريتشارد بوزنر) Richard Posner بأن خط ميلر Miller للقضايا "غير واقعي unrealistic"[65]. ذلك ان "الخصوصية المعلوماتية لا تعني رفض مشاركة المعلومات مع الجميع"، كما يؤكد، لأنه "يجب ألا نخلط بين الانعزال solitude والسرية secrecy"[66]. وتوافق (شيري كولب) Sherry Colb على ذلك، حيث كتبت أن "التعامل مع التعرض لجمهور محدود على أنه مطابق للتعرض للعالم"[67] يفشل في التعرف على درجات الخصوصية degrees of privacy.

2. النقد الوظيفي

2. The Functional Critique

ويؤكد النقد الرئيسي الثاني لفقه الطرف الثالث أنه يمنح الحكومة سلطة أكبر مما يتفق مع مجتمع حر ومفتوح. يبدو أن أول تفصيل مهم لهذه الحجة هو معارضة dissent القاضي (هارلان) Justice Harlan في قضية وايت[68]. جادل القاضي (هارلان) بأنه لا ينبغي السماح للحكومة باستخدام مخبر سري undercover informant يضع سلك تصنت Wire لأن ترك مثل هذا الإجراء دون تنظيم من شأنه أن يمنح الحكومة الكثير من السلطة:

إذا كان التنصت من طرف ثالث ممارسة سائدة، فقد يخنق تلك العفوية- التي تنعكس في الخطاب التافه والمتهور والمدنس والمتحدي- الذي يحرر الحياة اليومية. ويمكن نسيان الكثير من التبادل غير المباشر بسهولة ويمكن للمرء أن يعتمد على غموض ملاحظاته، المحمية بحقيقة وجود جمهور محدود، واحتمال أن المستمع إما أن يتجاهل أو ينسى ما يقال، وكذلك عدم قدرة المستمع على إعادة صياغة محادثة دون الحاجة إلى التعامل مع سجل موثق. كل هذه القيم يتم التضحية بها من خلال سيادة القانون التي تسمح بالمراقبة

[62] Smith, 442 U.S. at 750 (Marshall, J., dissenting).
[63] See, e.g., Katz, supra note 5, at 564–66.
[64] Smith, 442 U.S. at 749 (Marshall, J., dissenting). Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083, 1086 (2002).
[65] Richard A. Posner, Not A Suicide Pact: The Constitution in a Time of National Emergency 140 (2006).
[66] Id.
[67] Sherry F. Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119, 122 (2002).
[68] United States v. White، 401 U.S. 745 (1971).

الرسمية للخطاب الخاص التي لا تحدها سوى الحاجة إلى العثور على مساعد راغب willing assistant [69].

أثارت معارضة القاضي (مارشال) Justice Marshall في قضية Smith [70] نقطة مماثلة. وفقا (لمارشال) According to Marshall، فإن إعفاء سجلات القلم exempting pen registers من تدقيق scrutiny التعديل الرابع مكن من المراقبة غير المنظمة التي من شأنها أن تضر بالمجتمع الحر:

ومما لا شك فيه أن احتمال المراقبة الحكومية غير المنظمة سيثبت أنه مزعج حتى لأولئك الذين ليس لديهم أي شيء غير قانوني لإخفائه. قد يرغب العديد من الأفراد، بمن فيهم أعضاء المنظمات السياسية التي لا تحظى بشعبية أو الصحفيون الذين لديهم مصادر سرية، بشكل مشروع في تجنب الكشف عن اتصالاتهم الشخصية. وبالتالي، فإن السماح للحكومة بالوصول إلى سجلات الهاتف لسبب أقل من المحتمل قد يعيق أشكالا معينة من الانتماء السياسي والمساعي الصحفية التي تشكل السمة المميزة لمجتمع حر حقا[71].

التقط (أرنولد لوي) Arnold Loewy هذا الموضوع في دراسته عام 1983، التعديل الرابع كأداة لحماية الأبرياء The Fourth Amendment as a Device for Protecting the Innocent [72]. حيث افترض (لوي) أن حماية التعديل الرابع يجب أن تمتد الى الأبرياء، ثم استنتج أن قضايا فقه الطرف الثالث أعطت الشرطة الكثير من السلطة لمضايقة المواطنين الأبرياء[73]. من خلال السماح للعملاء السريين بتسجيل المشتبه بهم دون تدقيق قضائي judicial scrutiny، اذ منحتهم المحكمة "القدرة على استخدام برنامج تسجيلات القلم [pen registers] لألعاب الصالون أو النكات العملية أو المضايقة"[74]. من خلال السماح للشرطة بتركيب سجلات القلم دون إشراف، فقد تركت المحكمة الشرطة "حرة تماما في معرفة كل رقم هاتف يتصل به أي شخص [هكذا]، رهنا فقط بتعاون شركة الهاتف"[75].

وقد أثار علماء آخرون نقاطا مماثلة[76]، وفي كثير من الأحيان في مناقشات حول كيفية تطبيق التعديل الرابع على أجهزة الحاسوب والإنترنت. خدمات الإنترنت هي خدمات طرف ثالث، مما يزيد من احتمال أن التعديل الرابع قد ينطبق بشكل متواضع فقط على اتصالات الإنترنت. رد العلماء بالقول إن فقه الطرف الثالث "لا تستجيب للحياة في عصر المعلومات الحديث"[77]. وإذا لعبت خدمات الطرف الثالث دورا متزايدا في المراقبة الحكومية، فإن القلق مستمر، فإن التعديل الرابع سينظم جزءا أصغر وأصغر من تلك المراقبة؛ ستكون الحكومة قادرة على جمع وتجميع "الملفات الرقمية digital dossiers" دون تدقيق التعديل الرابع[78].

---

[69] See id. at 787–89 (Harlan, J., dissenting) (footnotes omitted).
[70] Smith v. Maryland, 442 U.S. 735, 748–52 (1979) (Marshall, J., dissenting).
[71] Id. at 751 (citations omitted).
[72] Loewy, supra note 5.
[73] Id. at 1252–56.
[74] Id. at 1253.
[75] Id. at 1255.
[76] See, e.g., Katz, supra note 5, at 568–69 (“The government is free from any judicial oversight. Without a reasonableness limitation, we must rely on government officials to voluntarily respect our privacy.”)
[77] Solove, supra note 64, at 1087.
[78] Id.; Joseph T. Thai, Is Data Mining Ever a Search Under Justice Stevens’s Fourth Amendment? 74 Fordham L. Rev. 1731, 1736–45 (2006).

ولضمان الحماية الدستورية الكافية عبر الإنترنت، يجادل الكثيرون بأنه يجب نقض قضايا الأطراف الثالثة أو قصرها بشكل حاد على حقائقها[79].

II. تأثير الاستبدال والأداة الوظيفية لفقه الطرف الثالث

II. Substitution Effects and the Functional Role of the Third-Party Doctrine

إن الانتقاد الواسع النطاق لمبدأ الطرف الثالث يتجاهل فائدتين مهمتين للقاعدة. يشرح هذا الجزء الفائدة الرئيسية الأولى لفقه الطرف الثالث: فهو يضمن الحياد التكنولوجي technological neutrality في قواعد التعديل الرابع. واستخدام أطراف ثالثة له تأثير استبدال substitution effect. إنه يتيح للمخطئين enables wrongdoers من أخذ الجوانب العامة لجرائمهم واستبدالها بمعاملات خاصة. بدون عقيدة طرف ثالث، يمكن للمشتبه بهم التصرف بشكل انتهازي لإخفاء مؤسساتهم الإجرامية بشكل فعال عن المراقبة. النتيجة تخل بالتوازن الأساسي لقانون التعديل الرابع، مما يقوض القوة الرادعة والعقابية للقانون الجنائي. وتمنع عقيدة الطرف الثالث مثل هذه الجهود، مما يؤدي إلى تكافؤ تقريبي في المقدار الإجمالي للخصوصية للمجرمين الذين يتصرفون بمفردهم ومقدار الخصوصية لأولئك الذين يستخدمون أطرافا ثالثة.

لتطوير هذه الحجة، سأبدأ بالتوازن الأساسي للتعديل الرابع. سأشرح كيف تهدد الأطراف الثالثة هذا التوازن وكيف تحتفظ بفقه الطرف الثالث به. وسأغطي بعد ذلك بعض الأمثلة وأختتم بإظهار كيف أن الفقه هو جانب أساسي من الحياد التكنولوجي لقواعد التعديل الرابع.

A. التقسيم الأساسي للتعديل الرابع

A. The Basic Division of the Fourth Amendment

يستند حظر التعديل الرابع لعمليات التفتيش searches والمصادرة seizures غير المعقولة unreasonable إلى التوازن بين الخصوصية والأمن. ولتنفيذ هذا التوازن، أنشأت المحكمة العليا فئتين أساسيتين من مسلك السلطات enforcement conduct: خطوات التحقيق التي ينظمها التعديل الرابع وتلك التي لا ينظمها.

بموجب هذا المخطط، يحمي التعديل الرابع بعض الأشياء وبعض الأماكن بينما يترك البعض الآخر مفتوحا للمراقبة الحكومية. على سبيل المثال، يحمي التعديل الرابع منزل الشخص والطرود الخاصة private packages [80]. إذا أرادت الحكومة الوصول إلى تلك الأماكن، فيجب أن يكون لديها عادة أمر تفتيش[81]. من

---

[79] E.g., Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375, 1403 (2004) (articulating that the third-party doctrine should be construed narrowly in the context of computer and internet communications); Freiwald, supra note 5, at ¶ 40; Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557 (2004) (arguing that the third-party doctrine should be read narrowly in the case of computer and internet communications).

[80] E.g., Payton v. New York, 445 U.S. 573, 585 (1980) (noting that the " 'chief evil against which the Fourth Amendment is directed' " is the warrant-less entry and search of a home (quoting United States v. United States Dist. Court, 407 U.S. 297, 313 (1972))).

[81] Id.

ناحية أخرى، فإن الأحداث في الأماكن العامة أو المفتوحة غير محمية بموجب التعديل الرابع[82]. إذا أرادت الحكومة مراقبة مثل هذه المساحات، فإن التعديل الرابع لا يتدخل: المراقبة ليست تفتيشا أو مصادرة .monitoring is not a search or seizure.

يشكل تقسيم التعديل الرابع بين المساحات غير المنظمة والمنظمة جزءا أساسيا من كيفية عمل التعديل. ويقسم جمع الأدلة إلى مرحلتين: خطوات أقل توغلا يمكن للحكومة اتخاذها في أي وقت، وخطوات أكثر توغلا لا يمكن للحكومة اتخاذها إلا عندما تكون قد جمعت بالفعل أدلة كافية لإثبات ظروف خاصة مثل السبب المحتمل أو الظروف الملحة.

من وجهة نظر التحقيق، تعمل الفئتان معا. غالبا ما تبدأ التحقيقات بالمراقبة المفتوحة، مما يسمح للشرطة بالبحث عن أدلة قد تشير إلى نشاط إجرامي. وإذا أسفرت المراقبة العلنية عن أدلة كافية، فإن هذه الأدلة تسمح للحكومة باتخاذ خطوات أكثر تدخلا غالبا ما تكون ضرورية لإثبات القضايا بما لا يدع مجالا للشك في المحكمة[83].

يؤدي التقسيم الأساسي إلى خطوات غير منظمة ومنظمة إلى توازن بين الخصوصية والأمن balance between privacy and security لأن معظم الجرائم تتطلب تقليديا من المشتبه بهم تنفيذ جزء على الأقل من جرائمهم في أماكن مفتوحة للمراقبة. ولمعرفة السبب، فكر في عالم بدون تكنولوجيا متقدمة. عادة ما يحدث جزء من الجريمة في الخارج. إذا أراد جون سرقة شخص يسير في الشارع، على سبيل المثال، فعليه مغادرة منزله والخروج إلى الشارع. وإذا أراد شراء المخدرات، فعليه الخروج من منزله والعثور على تاجر يبيعها له. ثم إذا أراد قتل زميله في العمل، فعليه الخروج وشراء سكين. ثم بعد الفعل/ السلوك act، يحتاج إلى التخلص من الجثة body. في كل هذه الأنواع التقليدية من الجرائم، يتعين على الجاني مغادرة منزله والخروج إلى أماكن غير محمية unprotected بموجب التعديل الرابع.

والعنصر العام لمعظم الجرائم التقليدية أمر بالغ الأهمية للتوازن التقليدي لقواعد التعديل الرابع. إذا حدث جزء على الأقل من الجريمة في أماكن غير محمية بموجب التعديل الرابع، فإن الشرطة لديها على الأقل بعض الفرص للنظر عن كثب فيما إذا كان النشاط الإجرامي على قدم وساق. نظرا لأن الشرطة تبدأ عادة تحقيقا مع تكهنات فقط بأن شخصا معينا ينتهك القانون، فإن الجزء العام من الجرائم يمنح الشرطة فرصة لتطوير المزيد من الأدلة. وستتاح للشرطة إمكانية الوصول إلى الجزء العام من الجريمة دون تنظيم قانوني. إذا كانوا يراقبونه، فسيعرفون أين ذهب المشتبه به وماذا قال علنا public.

هذه المعلومات لن تحل الجريمة في معظم الحالات: ما لم يراقب الضابط الجريمة مباشرة، فإن الأدلة المتاحة للجمهور لا توفر سوى دليل.84 لكنها بداية. إذا كانت الأدلة قوية بما فيه الكفاية، فيمكنها دعم غزو المساحات المحمية بأمر قضائي. وتساعد هذه الخطوات الشرطة على حل نسبة معتدلة على الأقل من القضايا الجنائية. بالطبع، لن يتم حل العديد من الحالات. ولكن يتم حل عدد كاف من الحالات بحيث يوجد احتمال كبير للعقوبة الجنائية، مما يسمح لنظام العدالة الجنائية بخدمة غاياته النفعية والعقابية.

[82] California v. Ciraolo, 476 U.S. 207, 213 (1986) (“The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.”).
[83] In the argot of existing doctrine, government conduct that violates a reasonable expectation of privacy is a “search” that ordinarily triggers the warrant requirement; other government conduct is not a “search” at all.

B. الأطراف الثالثة والتقسيم الأساسي

B. Third Parties and the Basic Division

تشكل الأطراف الثالثة تهديدا كبيرا للتقسيم الأساسي للتعديل الرابع بين الخطوات غير المنظمة والمنظمة. والسبب هو أن الأطراف الثالثة تعمل كوكلاء عن بعد يسمحون للمخالفين بارتكاب الجرائم بالكامل على انفراد. أولئك الذين يرتكبون الجرائم يحاولون بطبيعة الحال إخفاءها عن الشرطة. لا يوجد مجرم يريد أن يتم القبض عليه. إذا كان بإمكان مرتكب الفعل غير المشروع استخدام أطراف ثالثة كوكلاء عن بعد، فيمكنه تقليل تعرضه للمراقبة العامة. بدلا من الخروج إلى العالم وتعريض نفسه للتعرض، يمكن للظالمين إحضار وكلاء من جهات خارجية إلى الداخل ومشاركة الخطط أو تفويض المهام إليهم. يمكنه استخدام خدمات الطرف الثالث لارتكاب جرائمه دون تعريض نفسه لمساحات مفتوحة للمراقبة الحكومية.

بعبارة أخرى، غالبا ما يكون لاستخدام أطراف ثالثة تأثير استبدال[84]. بدون الطرف الثالث، كان على المخطئ أن يخرج إلى الأماكن العامة حيث لا ينظم التعديل الرابع المراقبة. لكن استخدام طرف ثالث يحل محل معاملة خفية للحدث المفتوح سابقا. ما كان يمكن أن يكون علنيا أصبح الآن مخفيا. لم يعد الجاني بحاجة إلى مغادرة منزله، لأن وكلاء الطرف الثالث يمكنهم من ارتكاب الجريمة عن بعد. فالجريمة الآن تعود إلى المجرم بدلا من أن يذهب المجرم إلى الجريمة[85].

C. امثلة

C. Examples

تساعد الأمثلة في توضيح كيفية قيام الأطراف الثالثة بإنشاء تأثير استبدال وكيف يحافظ فقه الطرف الثالث على نفس الدرجة من حماية الخصوصية بغض النظر عما إذا تم استخدام أطراف ثالثة أم لا. على وجه الخصوص، ضع في اعتبارك التطبيقين الأكثر إثارة للجدل لفقه الطرف الثالث: سجل القلم pen register المثبت فيقضية سميث[86]، وسجلات الحساب المصرفي المستردة في الولايات المتحدة ضد ميلر[87].

[84] In the argot of existing doctrine, government conduct that violates a reasonable expectation of privacy is a “search” that ordinarily triggers the warrant requirement; other government conduct is not a “search” at all.
[85] Of course, this is not true in every case: It is possible to imagine an entirely private crime such as attempting suicide. But in most cases, some exposure is necessary.
[86] Smith v. Maryland, 442 U.S. 735 (1979).
[87] United States v. Miller, 425 U.S. 435 (1976).

1. قضية سميث ضد ماريلاند- سجل القلم

1. Smith v. Maryland—Pen Registers

أذكر أنه في قضية سميث ضد. ماريلاند[88]، ضايق harassed سميث ضحية سرقة robbery victim من خلال الاتصال بها مرارا وتكرارا repeatedlyعلى الهاتف. واشتبهت الشرطة في سميث، وطلبوا من شركة الهاتف تثبيت جهاز تسجيل قلم pen register من شأنه أن يلاحظ أي مكالمات صادرة من هاتف منزله. سجل سجل القلم حقيقة المكالمة مع الضحية، مما يشير إلى أن سميث كان المتحرش ويساعد في تزويد الشرطة بسبب محتمل لأمر بتفتيش منزله.

لفهم تأثير الاستبدال هنا، نحتاج إلى أن نرى بالضبط كيف استخدم سميث الطرف الثالث third party من نظام الهاتف للتخلص من الجانب العام لجريمته. ففي عالم بدون نظام هاتف، كان سميث سيضطر إلى مطاردة ضحيته بالطريقة القديمة. كان سميث سيغادر منزله، ويمشي إلى سيارته، ويقود سيارته إلى منزل ضحيته لمضايقتها شخصيا. بدلا من جعل شركة الهاتف تقوم بتثبيت سجل قلم، كانت الشرطة ستعين ضابطا لمراقبة سميث من الشوارع العامة و "تتبعه tail" في جميع أنحاء المدينة. كان الضابط سيشاهد سميث يغادر منزله، ويدخل سيارته، ويقود سيارته إلى منزل الضحية.

عندما نقدم الطرف الثالث من نظام الهاتف، لم يعد سميث بحاجة إلى مغادرة المنزل. وباستعارة الحملة الإعلانية القديمة للصفحات الصفراء، يمكنه "السماح لأصابعه بالمشي"[89]. وما كان سيحدث سابقا في الهواء الطلق يحدث الآن داخل المنزل باستخدام الطرف الثالث من الهاتف. بدلا من مشاهدة سميث في الأماكن العامة، تحتاج الشرطة الآن إلى تثبيت سجل قلم للحصول على ما يعادل المعلومات العامة السابقة حول ما كان يفعله.

المعلومات العامة السابقة حول ما كان يفعله. ومن هذا المنظور، فإن قرار المحكمة العليا في قضية سميث تمنع ولاية ماريلاند بشكل صحيح من محاولة سميث في النهاية حول توازن قواعد التعديل الرابع. حيث ان استنتاجها بأن تثبيت سجل القلم ليس بحثا يطابق حماية التعديل الرابع لجرائم الطرف الثالث مع الحماية الموجودة مسبقا للجرائم الفردية. فقد أدى استخدام سميث لطرف ثالث إلى سحب هويته من المراقبة العامة: بدلا من الاضطرار إلى السفر إلى ضحيته، جلب الهاتف ضحيته إليه (افتراضيا، على الأقل).

حلت معلومات سجل القلم pen register information محل نفس المعلومات التي كانت الشرطة ستحصل عليها من خلال مشاهدة سميث في الشارع العام. لم يكن وجود سميث المادي محميا في نسخة العالم المادي physical world للجريمة. وبموجب مبدأ الطرف الثالث، فإن وجوده الافتراضي غير محمي في بيئة الطرف الثالث لشبكة الهاتف[90].

---

[88] Smith, 442 U.S. at 737–38

[89] Paul R. La Monica, Let your fingers do the walking, CNNMoney.com, December 13, 2005, http://money.cnn.com/2005/12/13/news/fortune500/yellow.

[90] During the editing stage, I learned that Ric Simmons recently made a similar argument about Smith. See Ric Simmons, Why 2007 Is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence, 97 J. Crim. L. & Criminology 531, 553– 54 (2007). Simmons and I share a similar approach to how technology impacts Fourth Amendment protection; both of us have emphasized how technological change can both take away government power and expand it, and how Fourth Amendment rules respond to changes in both directions. See Orin S. Kerr, The Fourth Amendment

2. قضية ميلر- سجلات البنوك

2. United States v. Miller—Bank Records

بعد ذلك، ضع في اعتبارك قضية الولايات المتحدة ضد. ميلر[91]، واستنتاجها/ تقريرها بعدم وجود حماية التعديل الرابع للسجلات المصرفية bank records. فمن الصعب إلى حد ما رؤية تأثير الاستبدال substitution effect في هذه الحالة، لكنني أعتقد أنه لا يزال يفسر النتيجة. ففي ميلر، أرادت الحكومة إثبات أن ميلر قد أقام كحولا غير مشروع illegal alcohol still. فاستخدم المدعون العامون Prosecutors سجلات ميلر المصرفية لإظهار أنه اشترى معدات لحسابه الجاري الذي لا يزال يستخدمه[92]. وبعبارة أخرى، استخدمت الحكومة الحساب الجاري لإثبات التجارة: أموال ميلر، المسحوبة drawn من البنك، مقابل العناصر التي كان يشتريها لبناء العقار still. رأت المحكمة العليا أن التعديل الرابع لا يحمي سجلات ميلر المصرفية. على وجه التحديد، لم يحمي من التدقيق الحكومي الشيكات التي كان على ميلر كتابتها لإجراء تلك الصفقات[93].

ففي قضية ميلر، خلق الحساب الجاري تأثيرا بديلا عن طريق استبدال معاملة كانت ستشمل مكونات عامة كبيرة بمعاملة تحدث عادة بالكامل في القطاع الخاص. لنرى كيف، تخيل عالما بدون بنوك. إذا كنت بحاجة إلى الدفع مقابل شيء ما في هذا العالم، فستحتاج إلى الحصول على المال للقيام بذلك: ستحتاج إلى التنقل إلى

---

and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 864–67 (2004); Simmons, supra, at 535–36. Simmons ultimately condemns the third-party doctrine, calling it "dangerously short-sighted," but that is because he assumes that the doctrine must also apply to the contents of communications. Simmons, supra, at 555. As I explain in Section II.D, I do not think the third-party doctrine needs to apply to contents of communications. With that caveat, I agree with the basic approach of Professor Simmons.

خلال مرحلة التحرير، علمت أن ريك سيمونز قدم مؤخرا حجة مماثلة عن سميث. انظر ريك سيمونز، لماذا 2007 ليس مثل عام 1984: منظور أوسع للتكنولوجيا التأثير على الخصوصية وفقه التعديل الرابع. أنا وسيمونز نتشارك نهجا مشابها لكيفية تأثير التكنولوجيا على التعديل الرابع حماية; لقد أكد كلانا كيف يمكن للتغير التكنولوجي أن يسلب الحكومة السلطة وتوسيعها، وكيف تستجيب قواعد التعديل الرابع للتغييرات في كلا الاتجاهين. رأى أورين س. كير ، التعديل الرابع والتقنيات الجديدة: الأساطير الدستورية وقضية تحذير، وسيمونز في النهاية يدين فقه الطرف الثالث، واصفا إياه بأنه "قصير النظر بشكل خطير" ، ولكن هذا لأنه يفترض أن المبدأ يجب أن ينطبق أيضا على محتويات الاتصالات. كما أوضحت في القسم ثانيا - د، ولا أعتقد أن فقه الطرف الثالث يجب أن ينطبق على محتويات الاتصالات. ومع هذا التحذير، أتفق مع النهج الأساسي للبروفيسور سيمونز.

[91] United States v. Miller, 425 U.S. 435 (1976).

[92] Specifically, Miller had written a check to rent a van and purchase radio equipment, sheet metal, and metal pipe. See id. at 438.

[93] The Miller court explained: The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

وأوضحت محكمة ميلر ما يلي: يخاطر المودع، في الكشف عن شؤونه لآخر، بأن المعلومات ستكون التي نقلها ذلك الشخص إلى الحكومة. وقد رأت هذه المحكمة مرارا وتكرارا أن التعديل الرابع لا يمنع التعديل الحصول على المعلومات التي يتم الكشف عنها لطرف ثالث ونقلها إلى السلطات الحكومية، حتى لو تم الكشف عن المعلومات على افتراض أنه سيتم استخدامه فقط لغرض محدود وأن الثقة الموضوعة في الطرف الثالث سوف لا تتعرض للخيانة.

مأواك، والتقاط المال، ثم الانتقال إلى المكان الذي تجري فيه عملية الشراء. فإذا كنت البائع، فأنت بحاجة إلى استلام الأموال وإعادتها إلى مأواك وتخزينها بعيدا لحفظها safekeeping.

هناك أجزاء عامة من الصفقة على كلا الجانبين. الشيكات وأدوات الائتمان الأخرى تلغي الحاجة إلى السفر. لم يعد المشتري بحاجة إلى السفر لإحضار المال إلى البائع، ولم يعد البائع بحاجة إلى السفر لوضع المال بعيدا. بدلا من ذلك، يقوم البائع بإيداع الشيك ويتم إرسال الأموال من البنك إليه مباشرة. ولا يتعين على المشتري والبائع الانتقال بعد الآن، حيث يقوم الشيك بنقل الأموال من وإلى حساباتهم دون الحاجة إلى الذهاب إلى أي مكان. الطرف الثالث من الحساب الجاري يجعل المعاملة الاقتصادية بأكملها خاصة.

إن استخدام مبدأ الطرف الثالث في قضية ميلر أمر معقول لأن خدمات التحقق تحل محل المعاملات العامة بشكل كبير بأخرى خاصة. حيث يضمن مبدأ الطرف الثالث تطبيق نفس قواعد التعديل الرابع على التحقق من معاملات الحساب التي كانت ستنطبق على المعاملات العامة التي تحل محلها.

D. الطرف الثالث والحياد التكنولوجي

D. Third Parties and Technology Neutrality

انا أدرك أن النموذج أعلاه مصطنع بعض الشيء. إنه يتخيل عاما أسطوريا لا توجد فيه أطراف ثالثة، سواء من النوع البشري أو الالي/ الميكانيكي. ومن الواضح أنه لم يكن هناك مثل هذا الوقت. حيث يتخيل النموذج أعلاه أيضا أن تأثير الاستبدال سيحدث بالتساوي في كل حالة. ولن يحدث ذلك: يمكن للمجرمين استخدام أطراف ثالثة لسحب الجزء العام من جرائمهم، لكن بالتأكيد لا يتعين عليهم القيام بذلك. ففي قضية سميث، على سبيل المثال، كان بإمكان سميث إجراء مكالمة المطاردة المجهولة من هاتف عمومي مدفوع الأجر. أو، في المعادل الحديث، كان بإمكانه استخدام هاتف محمول في شارع مزدحم بالمدينة والتحدث بصوت عال حتى يتمكن الجميع من سماعه. إذا كان قد فعل ذلك، فإن استخدام طرف ثالث لم يكن ليغير الجانب المفتوح للجريمة.

وفي الوقت نفسه، يكشف النموذج المبسط إلى حد ما عن دينامية أساسية بشأن استخدام أطراف ثالثة: وبوجه عام، يمكن أن يؤدي استخدام طرف ثالث إلى إحداث أثر استعاضة حيثما يرغب مرتكب الفعل غير المشروع في أن يفعل ذلك. يمكن أن يختار (هوفا) التحدث فقط إلى زملائه المقربين في أمان غرفته في الفندق. يمكن أن يختار سميث الاتصال بضحيته فقط من هاتف منزله. لا يكون لاستخدام طرف ثالث دائما تأثير استبدالي substitution effect، ولكنه يتيح التأثير حسب اختيار المشتبه فيه. وأي مجرم ذكي سيمارس الخيار. أولئك الذين لديهم أكثر ما يخفونه لديهم أكبر حافز للاستفادة من كيفية إخفاء خدمات الجهات الخارجية لنشاطهم. حتى بدون قواعد التعديل الرابع، ستميل خدمات الجهات الخارجية إلى إخفاء المعاملات العامة بخلاف ذلك. سيستخدم الفاعل العقلاني المصمم على السلوك الإجرامي أكبر عدد ممكن من خدمات الجهات الخارجية لتجنب اكتشافه.

من هذا المنظور، فإن عقيدة الطرف الثالث ليست نوعا من الثقب الغامض في حماية التعديل الرابع. بل على العكس من ذلك، فهو تناظر طبيعي لقرار المحكمة العليا في قضية (كاتز) ضد الولايات المتحدة[94]. فقد اشترط (كاتز) الحياد التكنولوجي technological neutrality بشكل فعال: على الرغم من أن منطقه الدقيق غير

[94] Katz v. United States, 389 U.S. 347 (1967).

شفاف opaque، إلا أنه غالبا ما يفهم على أنه استنتاج مفاده أن المكالمات الهاتفية محمية بسبب الوظيفة التي تخدمها بدلا من وجود التكنولوجيا التي تستخدمها[95]. وفي الواقع، كان هذا هو الأساس المنطقي الأساسي لمعارضة القاضي (براندیز) Justice Brandeis في قضية أولمستيد ضد الولايات المتحدة[96].

لقد خشي القاضي (براندیز) من أن التغيير التكنولوجي يمكن أن يضيق حماية التعديل الرابع: "قد يتم تطوير طرق يمكن للحكومة في يوم من الأيام، دون إزالة الأوراق من الأدراج السرية، إعادة إنتاجها في المحكمة، والتي سيتم من خلالها تمكينها من الكشف أمام هيئة محلفين عن أكثر الأحداث حميمية في المنزل "[97]. ولقد اقترح القاضي (براندیز) أن التعديل الرابع يجب أن يواكب تغير التكنولوجيا حتى لا تؤدي التقنيات الجديدة إلى الإضرار بالخصوصية.

ولكن إذا تبنينا هذا الفهم للتعديل الرابع، فمن المؤكد أنه يجب أن يكون طريقا ذا اتجاهين. وكما يمكن للتكنولوجيات الجديدة أن تخرج "الأحداث الحميمة للمنزل intimate occurrences of the home " إلى العلن out in the open، كذلك يمكن للتغير التكنولوجي واستخدام أطراف ثالثة أن يأخذا المعاملات التي كانت في العلن ويجلبانها إلى الداخل. وإذا قبلنا أن التعديل الرابع يجب أن يظل محايدا من الناحية التكنولوجية، فعلينا أن نقبل هذه القاعدة عندما تهدد الممارسات التكنولوجية الجديدة بتوسيع حماية التعديل الرابع كما هو الحال عندما تهدد بتقييدها.

مثلما يجب أن يحمي التعديل الرابع ما تكشفه التكنولوجيا، كذلك يجب أن يسمح التعديل الرابع بالوصول إلى ما تخفيه التكنولوجيا. من هذا المنظور، فهناك حاجة إلى فقه الطرف الثالث لضمان الحياد التكنولوجي للتعديل الرابع. حيث إنه يضمن أن لدينا نفس الدرجة التقريبية rough degree من حماية التعديل الرابع بغض النظر عما إذا كان المخطئون wrongdoers يستخدمون وكلاء طرف ثالث لتسهيل جرائمهم.

وعلى نطاق أوسع، فإن فقه الطرف الثالث لا يقوض بأي حال من الأحوال (كاتس) Katz، الذي اشتهر بأن محتويات مكالمة من هاتف عام تتلقى حماية التعديل الرابع. فلا تؤدي محتويات الاتصالات المرسلة عبر شبكات الجهات الخارجية إلى تأثيرات الاستبدال: فلا يخفي استخدام الشبكة المحتويات التي كانت مفتوحة سابقا. عندما يزور شخص آخر في منزله، تحدث حقيقة الزيارة علنا ولكن المحتويات الفعلية لمحادثاتهم تظل محمية من الملاحظة. وإن توسيع التعديل الرابع ليشمل محتويات الاتصالات مع استبعاد معلومات العنوان- كما فعلت المحكمة العليا في (كاتز وسميث)- يحافظ على هذا الوضع الراهن ويتبع نهجا محايدا تقنيا للحماية الدستورية.

---

[95] The Katz Court stated: One who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication. Id. at 352.
ولقد قررت محكمة كاتس: الشخص الذي يشغل [كشك الهاتف]، ويغلق الباب خلفه، ويدفع الرسوم التي تسمح له بإجراء مكالمة يحق له بالتأكيد أن يفترض أن الكلمات التي ينطق بها في لسان حال سوف لا يتم بثها للعالم. قراءة الدستور بشكل أضيق هو تجاهل للدور الحيوي أن الهاتف العام يلعب دورا في الاتصالات الخاصة. Id. at 352.

[96] Olmstead v. United States. 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

[97] "Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Id. at 474.

III. عقيدة الطرف الثالث والوضوح المسبق

III. The Third-Party Doctrine and Ex Ante Clarity

ان الدور الثاني المهم لفقه الطرف الثالث هو تعزيز الوضوح المسبق ex ante clarity في قواعد التعديل الرابع. حيث يتطلب مفتاح التشغيل / الإيقاف on/off switch لعلاج الرفض suppression قواعد واضحة للتعديل الرابع بشأن سلوك الشرطة الذي يؤدي إلى حماية التعديل الرابع وما لا يفعله سلوك الشرطة[98]. حيث يخلق مبدأ الطرف الثالث وضوحا مسبقا من خلال مطابقة قواعد التعديل الرابع للمعلومات مع قواعد التعديل الرابع للموقع. وبموجب هذا الفقه، تسقط الحقوق في المعلومات عندما تصل المعلومات إلى وجهتها. هذا يعني أن الموقع الحالي للمعلومات يحدد قواعد التعديل الرابع لجمعها، وقواعد التعديل الرابع ثابتة داخل كل موقع. وبدون فقه الطرف الثالث، فانه يتعين على المحاكم تطوير بعض الاختبارات البديلة، بنفس الوضوح المسبق، لتحديد متى تكون المعلومات محمية بموجب التعديل الرابع. فقد لا تكون هذه المهمة مستحيلة، ولكنها صعبة للغاية. حاول عدد قليل من منتقدي فقه الطرف الثالث ذلك. وصعوبة استنباط بديل واضحة لفقه الطرف الثالث فلم توفر حجة ثانية لصالحه.

A. الوضوح المسبق بموجب مبدأ الطرف الثالث

A. Ex Ante Clarity Under the Third-Party Doctrine

لفهم أهمية الوضوح المسبق، فانه من الضروري الاعتراف بأن قاعدة الاستبعاد توفر الآلية الأساسية لإنفاذ التعديل الرابع[99]. فإذا انتهكت الشرطة توقعا معقولا للخصوصية ولم يتم تطبيق أي استثناء، عادة قمع الأدلة التي يتم الحصول عليها وقد يطلق سراح مرتكب الخطأ[100]. وتتطلب التكاليف الباهظة لقاعدة الاستبعاد وضوحا مسبقا في القواعد عندما يكون هناك توقع معقول للخصوصية. حيث تحتاج الشرطة إلى معرفة متى يؤدي سلوكها إلى حماية التعديل الرابع. يمكن أن يؤدي عدم اليقين إلى ردع الشرطة عن التصرف عندما لا توجد حماية ويمكن أن يؤدي بهم إلى الدوس عن غير قصد على حقوق التعديل الرابع[101]. ويضمن فقه الطرف الثالث الوضوح المسبق من خلال مطابقة قواعد التعديل الرابع لجمع المعلومات مع موقع المعلومات التي تم جمعها. عندما تصل المعلومات إلى وجهتها، تتطابق قواعد التعديل الرابع لجمع المعلومات مع قواعد جمع الأدلة الأخرى هناك.

هذا صحيح لأن الحقوق في المعلومات تسقط عندما تصل المعلومات إلى وجهتها. اذ يتم الكشف عن المعلومات لمتلقيها، ولم تعد أي حماية موجودة مسبقا في التعديل الرابع موجودة[102]. وهذا النهج ضروري لوضوح قواعد التعديل الرابع لأنه يضمن أنه بمجرد وجود المعلومات في مكان ما، يتم التعامل معها تماما مثل أي شيء آخر موجود هناك. نظرا لأن تاريخ المعلومات يتم محوه عند وصوله، يمكن للقانون فرض

---

[98] See Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 527 (2007) ("The Fourth Amendment's suppression remedy . . . generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.").

[99] See id. at 527–28.

[100] See generally Mapp v. Ohio, 367 U.S. 643 (1961) (applying the Fourth Amendment's suppression remedy to the states through the Fourteenth Amendment).

[101] See Kerr, supra note 100, at 527–28.

[102] See supra Section II.A.

قواعد بشأن ما يمكن أو لا يمكن للشرطة فعله بناء على الموقع المعروف للبحث بدلا من التاريخ المجهول للمعلومات التي تم الحصول عليها.

ضع في اعتبارك رسالة تصل إلى البريد، ويتم فتحها، وتجلس على مكتب المستلم في المنزل في كومة من الرسائل الأخرى والأوراق الأخرى. تملي عقيدة الطرف الثالث أن يتم التعامل مع الرسالة تماما مثل جميع الأوراق الأخرى على المكتب. وللمرسل حقوق التعديل الرابع في الرسالة أثناء الإرسال، ولكن بمجرد وصولها إلى وجهتها، تختفي هذه الحقوق[103].

إذا كانت الشرطة ترغب في تفتيش المنزل والعثور على كومة من الأوراق بما في ذلك الرسالة، فإن قواعد التعديل الرابع التي يجب عليهم اتباعها سيتم تعيينها وفقا للقواعد المعتادة لعمليات البحث عن المنازل بدلا من القواعد الخاصة لكل قطعة من الورق يحددها تاريخ كل صفحة. من خلال محو تاريخ المعلومات لأغراض التعديل الرابع، ويضمن فقه الطرف الثالث التعامل مع جميع المعلومات في نفس الموقع بنفس الطريقة. هذا أمر بالغ الأهمية لأن الشرطة ستعرف عادة حالة المكان الذي تفتيشه ولكن ليس تاريخ العناصر الموجودة بداخله.

وتتجلى أهمية الوضوح المسبق الذي يوفره مبدأ الطرف الثالث في الصعوبة المدهشة في استحداث بدائل للمبدأ يمكن أن تحافظ على ذلك الوضوح. بموجب عقيدة الطرف الثالث، إذا أخبر A سرا ل B، فلن يكون ل A حقوق في حيازة B للمعلومات. ومع ذلك، إذا تم رفض مبدأ الطرف الثالث، فيجب أن تستمر حقوق A في تلك المعلومات على الرغم من أن B لديه المعلومات الآن بالإضافة إلى A.

بمعنى آخر، يجب أن تحتفظ المعلومات بتاريخ: يجب أن تأخذ قواعد التعديل الرابع التي تنطبق على المعلومات في الاعتبار مكان وجود المعلومات في الماضي وفي أي ظروف تم الاحتفاظ بها والكشف عنها. والسؤال هو، إلى أي مدى يجب أن تذهب هذه الحقوق؟ هل يجب أن تمتد إلى الأبد extend forever؟ ما الذي يجب أن يطفئها extinguish؟ بالنسبة للجزء الأكبر، تجاهل التعليق العلمي هذه المشكلة: معظم العلماء الذين ينتقدون العقيدة يفعلون ذلك دون أن يشرحوا فعليا الاختبار الذي يجب أن يحل محله[104]. ولكن إذا تطلب الأمر نظرية للتغلب على نظرية، فمن المؤكد أن الأمر يتطلب فقه للتغلب على فقه. واتضح أنه من الصعب للغاية ابتكار بديل لفقه الطرف الثالث من شأنه أن يوفر الوضوح المطلوب.

B. الوضوح المسبق في ظل بديل احتمالي

B. Ex Ante Clarity Under a Probabilistic Alternative

نظرا لوجود عدة طرق مختلفة لتحديد متى يكون توقع الخصوصية معقولا[105]، فمن المفيد التفكير في بديلين مختلفين different alternatives للحلول replace محل مبدأ الطرف الثالث. أحد البدائل هو ما أسميته النموذج الاحتمالي probabilistic model لحماية التعديل الرابع[106]. وبموجب هذا النهج، يعتمد

[103] See United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992).
[104] See, e.g., Solove, supra note 64, at 1083 (criticizing the third-party doctrine, but not proposing a clear alternative to it).
[105] See generally Kerr, supra note 100, at 503.
[106] See id. at 508–12.

ما إذا كان سلوك الحكومة ينتهك توقعا معقولا للخصوصية على تحقيق خاص بالحقائق حول ما إذا كان الشخص العاقل reasonable person يتوقع أن تظل المعلومات خاصة[107].

هذا تحقيق مستقبلي من وجهة نظر المشتبه به: السؤال هو ما إذا كان شخص عاقل في حالة المشتبه فيه يتوقع نشر المعلومات على نطاق واسع widely disseminated. وفي هذا القسم، سأشرح لماذا لا يمكن للنهج الاحتمالي أن يخلق الوضوح المطلوب. ومن شأن اتباع نهج احتمالي أن يضع التحقيق على مسألة غير معروفة إلى حد كبير؛ ستواجه الشرطة صعوبة في تطبيق التعديل الرابع لأنها عادة ما تكون غير قادرة على إعادة بناء ما إذا كان شخص ما يتوقع بشكل معقول الخصوصية في المعلومات التي تم جمعها.

تكمن الصعوبة الأساسية في تطبيق نهج احتمالي probabilistic approach على معلومات الطرف الثالث في أن تاريخ المعلومات غالبا ما يكون معقدا ويستحيل إعادة بنائه. تماما كما قد يكون كوب من الماء من صنبور حوض المطبخ عبارة عن مياه أمطار في الأمازون منذ آلاف السنين، فإن المعلومات اليوم غالبا ما يكون لها ماض طويل من الانتقال بين الأشخاص.

ما يعرفه الشخص ويفكر فيه يعكس ما رآه وشمه وسمعه ولمسه وشعر به. حيث تعكس تجاربنا ما كشفه لنا العالم. ويتوقف العديد من هذه التجارب على ما اعتقده الآخرون واختبروه قبلنا بوقت طويل: وأفكارنا هي مزيج من آراء الأجيال الماضية. كلماتنا هي عجينة من أنفسنا والآخرين وتجارب حياة العديد من الناس في وقت واحد. نتيجة لذلك، لا يمكننا صناعة نموذج لنقل المعلومات model information transmission كمسار بسيط من A إلى B. وانما بدلا من ذلك، سوف تكون معظم عمليات الإرسال رحلة متعرجة معقدة من A إلى B إلى C إلى D إلى E مع المنعطفات والمنحنيات على طول الطريق.

هذا التعقيد complexity يحول inhibits دون الوضوح المسبق ex ante clarity للشرطة لأنها ستجمع بالضرورة المعلومات في نهاية نشرها، في حين أن الأحكام المتعلقة بما إذا كان من المحتمل أن تكون الخصوصية ومتى يجب أن تصدر في المستقبل.

من وجهة نظر الفرد الذي يرسل المعلومات، الذي لديه فضول حول ما إذا كان سيحافظ على حقوقه، سيقيم ما إذا كان متلقي المعلومات يبدو جديرا بالثقة. قد يسأل عما إذا كان لدى المستلم سياسة خصوصية، وقد يسأل عما إذا كان قد فشل في الحفاظ على الخصوصية في الماضي للتنبؤ بما قد يحدث في المستقبل. لكن المحققين الجنائيين ليس لديهم هذا الترف. يجب عليهم دحرجة الشريط إلى الوراء، بدءا من الحاضر ومحاولة إعادة بناء الماضي. إن تحديد ما إذا كان توقع الخصوصية معقولا بالمعنى الاحتمالي هو أمر سياقي للغاية، وسيكون السياق مختلفا بشكل كبير في نقاط نقل مختلفة في تاريخ المعلومات. نتيجة لذلك، فإن قواعد التعديل الرابع التي يجب على الشرطة تطبيقها مسبقا يجب أن تتوقف على تفاصيل تاريخ المعلومات التي لا يمكنهم معرفتها مسبقا وقد لا يتمكنون من إعادة بنائها على الإطلاق.

مثال بسيط يوضح المشكلة. تخيل أن المدعي العام الفيدرالي هو قارئ منتظم لمدونة CorruptionWatch.com، وهي مدونة حول جرائم الفساد العام. في أحد الأيام يزور المدونة ويجد تعليقا مجهولا تركه قارئ مجهول: "سمعت أن السناتور (سميث) شوهد علنا اليوم وهو يودع شيكا بقيمة 50,000 ألف دولار من (جاك أبراموف) Jack Abramoff في حساب السناتور سميث الشخصي في بنك أميس.

[107] Id.

هل قام (أبراموف) برشوته؟ لا أحد يعرف؟ أرسل لي مراسلة إلكترونية على "SenatorSmithsSecrets@gmail.com".

يشعر المدعي العام بالفضول بشأن ما يعرفه المعلق commenter، ويريد استدعاء subpoena كاتب التعليق. ولكن ما هي قاعدة التعديل الرابع التي ستحكم مثل هذا الاستدعاء؟ بموجب مبدأ الطرف الثالث، فإن القاعدة هي القاعدة التقليدية لإصدار مذكرات الاستدعاء. وهنا فتاريخ المعلومات لا علاقة له بالقاعدة القانونية التي يجب اتباعها. ولكن تخيل عالما يتم فيه استبدال فقه الطرف الثالث الحالية بنموذج احتمالي probabilistic model. فجأة أصبحت قاعدة التعديل الرابع غير واضحة. لا نعرف ما إذا كان أمر الاستدعاء سيورط توقع السناتور سميث المعقول للخصوصية لأننا لا نعرف من هو المعلق أو كيف عرف ما يعرفه.

لنأخذ في الاعتبار خمسة احتمالات; في الأول، مؤلف التعليق هو صراف البنك الذي خدم السناتور سميث وساعده في إيداع الشيك. وفي الثاني، المؤلف هو عميل زميل في بنك أميس في الطابور خلف السناتور سميث الذي سمع السناتور سميث يعلن بصوت عال أنه كان هناك لإيداع شيك بقيمة 50,000 ألف دولار من (جاك أبراموف). وفي الثالث، كاتب العبارة هو سارق بنك اقتحم البنك ونظر في ملفات السناتور سميث. وفي الرابع، الكاتب هو (جاك أبراموف)، الذي يريد أن يضع السناتور (سميث) في ورطة حتى يتمكن من التفاوض على صفقة أفضل مع الفيدراليين. واخيرا وفي الخامس، الكاتب هو السناتور (سميث) نفسه، الذي كان فضوليا لمعرفة ما إذا كان أي شخص سيصدق القصة إذا نشرها على الإنترنت دون الكشف عن هويته.

في أي من هذه الحالات ينتهك أمر الاستدعاء توقع السناتور (سميث) المعقول للخصوصية بموجب نهج احتمالي probabilistic approach- أي عندما يستند التوقع المعقول للخصوصية إلى تقييم احتمالي probabilistic assessment لما إذا كان السناتور (سميث) يتوقع بشكل معقول أن يتم نشر سلوكه على نطاق واسع؟ ربما يكون الجواب هو أن الأول والثالث ينتهكان توقعا معقولا للخصوصية، والثاني والخامس لا ينتهكان، والرابع يعتمد على تفاصيل العلاقة بين (سميث وأبراموف). ولكن كيف يمكن للشرطة معرفة ذلك؟ إنهم بحاجة إلى معرفة ما سيتعلمونه قبل أن يتمكنوا من معرفة ما إذا كان سلوكهم ينتهك التعديل الرابع.

وهذا مجرد غيض من فيض. تصبح الأمور أكثر تعقيدا إذا اعترف التعديل الرابع بتاريخ المعلومات بعد السؤال المباشر المتمثل في أحدث "قفزة" من نقطة الراحة الأخيرة. على سبيل المثال، قد يخبر جو سرا لجين Jane، التي قد تشاركه مع بن، الذي قد يكتبه في مذكراته التي سرقتها سارة، والتي قد تنشرها على مدونة يقرأها (إيرل)، الذي قد يخبرها بثقة لمخبر حكومي government informant.

الآن اطرح السؤال: هل يعلم المخبر للمعلومات انه ينتهك توقعات أي شخص معقولة للخصوصية؟ نحن بحاجة إلى النظر إلى ما وراء (إيرل)، كما نحتاج أيضا إلى الإجابة على سؤال سارة وبن وجين وجو. ولهذه المسألة، نحتاج إلى معرفة كيف عرف جو السر في المقام الأول. نحتاج إلى تتبع المعلومات حتى اللحظة التي ظهر فيها أن توقع شخص ما المعقول للخصوصية قد يتم انتهاكه. وبالطبع يجب معرفة كل هذه المعلومات قبل الحصول عليها. بطريقة ما يجب أن تعرف الشرطة تاريخ المعلومات التفصيلية للمعلومات التي لم يروها بعد. بموجب مبدأ فقه الطرف الثالث، فاذا لم تعد هناك حاجة لطرح هذه الأسئلة الصعبة للغاية. فانه يصبح تاريخ المعلومات غير ذي صلة.

C. الوضوح المسبق مع مع سياسة بديلة نافذة

C. Ex Ante Clarity with a Policy-Based Alternative

ان البديل الثاني لمبدأ فقه الطرف الثالث الحالي هو ما أسميته النهج القائم على السياسة[108]. وفي ظل هذا النهج، يوجد توقع معقول للخصوصية عندما يكون من الأفضل، كمسألة سياسة، أن يتم تنظيم ممارسة/ نمطية معينة من خلال شرط أمر بدلا من أن تكون غير منظمة بموجب التعديل الرابع[109].

عندما تطبق المحاكم نموذجا للسياسة، فإنها تصنف القضية المعروضة عليها وتقرر ما إذا كان التوقع المعقول للخصوصية يجب أن يمتد كمسألة سياسة إلى تلك الفئة من الوقائع. ومن الواضح أن نهج وضع سياسة A policy approach يمكن أن يؤدي إلى مزيد من الوضوح أكثر من النهج الاحتمالي probabilistic method، لأنه يوفر وسيلة للمحاكم لوضع قواعد تنطبق على فئات القضايا. ومع ذلك، فإن إنشاء قواعد واضحة للتعديل الرابع تستند فقط إلى اعتبارات السياسة العامة يتبين أنه أمر صعب نسبيا.

وفي رأيي، هناك صعوبتان رئيسيتان في استخدام القواعد القائمة على السياسة لإنشاء قواعد واضحة على معلومات الطرف الثالث. المشكلة الأولى هي أن هناك المئات من التطبيقات المتميزة المحتملة لمبدأ الطرف الثالث، وستحتاج المحاكم إلى تطبيق نموذج السياسة على كل منها لتحديد ما إذا كان ينبغي حماية المعلومات. وفقه الطرف الثالث هو مقاس واحد يناسب الجميع. ليست هناك حاجة لتحقيق التوازن بين السياسات على أساس كل حالة على حدة. ولكن إذا حاولت المحاكم الانخراط في موازنة السياسات لكل نوع من أنواع السجلات، فسوف تضطر إلى حل كيفية تطبيق التوازن على مجموعة واسعة جدا من القضايا. فعلى سبيل المثال، قد يرغب العديد من النقاد في نقض ميلر، القضية التي تنطوي على سجلات مصرفية، أو سميث، وهي القضية التي تنطوي على الاثبات وفق سجلات القلم pen registers.

ولكن ماذا عن قواعد التعديل الرابع لسجلات بطاقات الائتمان؟ سجلات الكهرباء؟ سجلات عداد الغاز؟ سجلات الهاتف؟ سجلات الإنترنت؟ عناوين بروتوكول الانترنت IP؟ سجلات متجر الكتب؟ سجلات متجر الملابس؟ سجل سجلات المتجر؟ حسابات (اي تيونز)؟ عملاء سريون Undercover يرتدون أسلاكا للتتبع wires؟ عملاء سريون لا يرتدون أسلاكا؟ وإلى أن تتم تسوية كل مسألة من هذه المسائل من قبل المحاكم، لن يكون لدى الوكلاء أية وسيلة لمعرفة كيف يحكم القانون الوصول إلى هذه المعلومات.

ثانيا، نظرا لأن العديد من تطبيقات فقه الطرف الثالث تنطوي على تطوير تقنيات، فإن نتيجة التحديد القائم على السياسة لكيفية تطبيق التعديل الرابع على معلومات الطرف الثالث يمكن أن تتغير بمرور الوقت[110]. ضع في اعتبارك كيف يمكن تطبيق التعديل الرابع على ما يسمى بمعلومات الرصد والتعقب trap-and-trace information: المعلومات التي يتم الحصول عليها من خلال جمع الحكومة لأرقام الهواتف الواردة لحساب هاتف معين[111].

[108] See id. at 519–22.
[109] Id.
[110] I have developed this argument in greater depth in Kerr, supra note 92, at 871–75.
[111] See generally 18 U.S.C. § 3127(4) (Supp. V 2005) (defining trap-and-trace devices for purposes of the Pen Register statute).

حتى انتشار خدمات "معرفة المتصل caller ID "، من المفترض أن معظم الأفراد اعتقدوا أن معلومات هوية المتصل خاصة. واليوم من ناحية أخرى، فإن الكشف عن رقم الهاتف الوارد هو ببساطة جزء قياسي من إجراء مكالمة هاتفية. يمكن أن يؤدي المعنى الاجتماعي المتغير لمعلومات الرصد والتتبع trap-and-trace information إلى خلق حالة من عدم اليقين uncertainty لمحققي الشرطة. إذا غيرت المحاكم إجابة التعديل الرابع مع تغير المعنى الاجتماعي social meaning، فكيف يمكن لضباط الشرطة معرفة متى سيحدث ذلك؟

وقد لا تكون هذه التحديات مستعصية على الحل. ربما يمكن للمحاكم وضع قواعد لتطبيق التعديل الرابع على كل من هذه الأنواع من السجلات. ربما تتغير الإجابات تدريجيا فقط ويمكن للمحاكم مواكبة ذلك بشكل جيد.

---

18 U.S. Code § 3121 - General prohibition on pen register and trap and trace device use; exception:

(a)IN GENERAL.—

Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(b)EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

(1)

relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2)

to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

(c)LIMITATION.—

A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d)PENALTY.—

Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

ولكن في الوقت نفسه، من المهم أن نرى أن إنشاء هذه المذاهب سوف يشكل في الواقع تحديا عمليا كبيرا. ولقد تجاهل جميع النقاد هذا باستثناء عدد قليل منهم. وعلى حد علمي، حاول البروفيسور (سلوبوجين) Slobogin فقط تقديم بديل شامل comprehensive alternative لفقه الطرف الثالث[112]. ولقد قدم البروفيسور (هندرسون) Henderson اختبارا لمجمل الظروف circumstances test المكون من تسعة عوامل[113]، ولكن العوامل factors وتطبيقها غامضة لدرجة أنها لا تقدم أي وضوح مسبق[114]. فإذا أراد النقاد استبدال فقه الطرف الثالث ببديل، فإنه ينبغي أن يكونوا أكثر وضوحا بشأن ماهية هذا البديل وكيفية تطبيقه في مجموعة واسعة من القضايا التي تواجهها المحاكم بانتظام.

IV. الاستجابة للانتقادات الموجهة لفقه الطرف الثالث

IV. Responding to Criticisms of the Third-Party Doctrine

إن عقيدة الطرف الثالث ليست حلا سحريا. أوضح القسم الأول- بأن العديد من منتقدي فقه الطرف الثالث قدموا حجتين أساسيتين ضدها، واحدة عقائدية والأخرى وظيفية. الادعاء العقائدي هو أن القضاة مخطئون عندما يؤكدون أن الشخص لا يحتفظ بتوقع معقول للخصوصية. وفقا لهؤلاء النقاد، غالبا ما يتوقع الناس بشكل معقول الخصوصية في معلومات الطرف الثالث الخاصة بهم[115]. ويسيء القضاة فهم الخصوصية لأنهم يفشلون في إدراك الفرق بين التعرض لشخص واحد والتعرض للجمهور. والحجة الثانية، الادعاء الوظيفي، هي أن عقيدة الطرف الثالث غير صحيحة لأنها تمنح الحكومة الكثير من السلطة. فهو يمنح الشرطة سلطة مطلقة للوصول إلى السجلات التجارية، واحتمال حدوث انتهاكات يجعل هذه السلطات غير متسقة مع المجتمع الحر وبالتالي مع التعديل الرابع[116].

يجادل هذا الجزء بأنه في حين أن كلا الانتقادين لهما بعض القوة، إلا أن كلاهما يبالغ إلى حد كبير في القضية ويتجاهل الحجج المضادة المهمة. أولا، ينتهي الأمر بالحجة العقائدية إلى أن تكون في الغالب حول الشكل بدلا من الجوهر. على الرغم من أن النقاد محقون في أن تطبيقات المحكمة لاختبار (كاتز) على العملاء السريين وسجلات الطرف الثالث محرجة، إلا أن هذا يرجع إلى حد كبير إلى أن قضايا الطرف الثالث تفهم بشكل أفضل على أنها قضايا موافقة. الكشف لأطراف ثالثة يلغي الحماية لأنه يعني الموافقة. عندما تفهم الحالات على أنها مجموعة فرعية من قانون الموافقة بدلا من كونها تطبيقات للتوقع المعقول لاختبار الخصوصية، ينتهي الأمر بالنقد العقائدي إلى أن يكون أضيق بكثير مما يقترحه النقاد.

تشير الحجج الوظيفية حول سلطة الحكومة بشكل صحيح إلى أن عقيدة الطرف الثالث تسمح بالممارسات الغازية التي يمكن إساءة استخدامها من قبل المسؤولين المفرطين في الحماس وحتى الفاسدين. ومع ذلك،

---

[112] Slobogin, supra note 5, at 179–96. I critique Professor Slobogin's proposal elsewhere in this Volume of the Michigan Law Review. Orin S. Kerr, Do We Need a New Fourth Amendment?, 107 Mich. L. Rev. (forthcoming April 2009) (reviewing Slobogin, supra note 5).

[113] Henderson, supra note 5.

[114] Professor Henderson's nine factors are (1) the purpose of the disclosure, (2) the personal nature of the information, (3) the amount of information, (4) the expectations of the disclosing party, (5) the understanding of the third party, (6) positive law guarantees of confidentiality, (7) government need, (8) personal recollections, and (9) changing social norms and technologies. Id. at 975.

[115] See supra Section I.B.1.

[116] See supra Section I.B.1.

فإنهم يتغاضون عن بدائل النظام القانوني العديدة لحماية التعديل الرابع. في غياب لائحة التعديل الرابع، وضعت الفروع الثلاثة قيودا على استخدام العملاء السريين والوصول إلى السجلات التجارية التي تعالج العديد من مخاوف النقاد.

تم تصميم امتيازات القانون العام Common law privileges، وقانون الرصد entrapment law، ومبدأ ماسايا Massiah doctrine، ومبدأ التعديل الأول، وحماية الخصوصية في التشريع statutory privacy protections خصيصا لمعالجة المخاوف من مضايقات الشرطة في استخدام أطراف ثالثة. وعلى الرغم من أن النقاد مبررون في خوفهم من الانتهاكات، إلا أنهم نظروا بشكل خاطئ إلى التعديل الرابع بمعزل عن غيره. تكشف المجموعة الكاملة من الردود القانونية على سجلات الطرف الثالث والعملاء السريين أن حماية التعديل الرابع ليست سوى واحدة من بين العديد من الأدوات القانونية لمعالجة هذه المخاوف. ونتيجة لذلك، فإن الحجة الوظيفية ضد فقه الطرف الثالث أضعف بكثير مما يتصور النقاد.

A. فقه الطرف الثالث كمبدأ الارادة

A. The Third-Party Doctrine as a Consent Doctrine

فكر أولاً في النقد العقائدي بأن المحكمة العليا غير صحيحة عندما تقول إن الأفراد لا يمكنهم الاحتفاظ بتوقع معقول للخصوصية في معلومات الطرف الثالث. وفي رأيي، ان النقاد العقائديون على حق جزئيا. فقد كانت تطبيقات المحكمة العليا للتوقع المعقول لاختبار الخصوصية لمعلومات الطرف الثالث محرجة awkward وغير مقنعة unconvincing. لكن السبب هو أن عقيدة الطرف الثالث تفهم بشكل أفضل كشكل من أشكال الموافقة/ الارادة Consent وليس كتطبيق لقضية (كاتز) Katz. حيث يؤدي إفصاح الطرف الثالث إلى إلغاء الخصوصية لأن الهدف يوافق طواعية على الكشف، وليس لأن استخدام الهدف لطرف ثالث يتنازل عن توقع معقول للخصوصية. الفرق دقيق ولكنه مهم من حيث المفهوم conceptually important، وأعتقد أنه يكشف أن النقد العقائدي doctrinal critique هو ادعاء أضيق بكثير مما يعتقد النقاد[117].

يمكن القول إن فكرة التعامل مع مبدأ الطرف الثالث كمشكلة موافقة تعود إلى إحاطة (هوفا) ضد الولايات المتحدة[118] في عام 1966، قبل عام من (كاتز). جادل موجز مزايا (هوفا) أمام المحكمة العليا بأن الخداع من قبل عميل سري، بارتين Partin، قد أبطل موافقة (هوفا). حيث تم خداع (هوفا) ، ولم تعد موافقته على السماح لبارتين بالاستماع صالحة قانونا: "خداع الحكومة في إخفاء المخبر تحت أدواره [النقابية] ... منع أي تنازل ذكي ومتفهم عن حقوق التعديل الرابع لمقدم الالتماس (هوفا) "[119]. رد موجز الحكومة بأن دافع بارتين لم يبطل الموافقة: لقد اعترف (هوفا) عن علم knowingly وقصد intentionally ببارتين في مساحاته الخاصة وشارك الأدلة على جريمته مع بارتين[120]. وبعد الموافقة على وجود بارتين، تنازل (هوفا) عن أي حقوق في التعديل الرابع[121].

---

[117] See supra Section I.B.2
[118] Hoffa v. United States. 385 U.S. 293 (1966).. All of these doctrines are discussed infra Part IV.
[119] "The Government's deception in hiding the informer under his [union] roles . . . prevented any intelligent and understanding waiver of Petitioner Hoffa's Fourth Amendment rights."
[120] Brief for Petitioners at 35–36, Hoffa v. United States, 385 U.S. 293 (1966) (Nos. 32, 33, 34, 35).
[121] Brief for the United States at 125–26, Hoffa, 385 U.S. 293 (Nos. 32, 33, 34, 35).

وكان ينبغي للمحكمة العليا أن تقبل هذه الصيغة القائمة على الموافقة لمبدأ الطرف الثالث. حيث حددت الأطراف في (هوفا) بدقة القضية التي أثارها مبدأ الطرف الثالث: **متى يشكل اختيار الشخص للكشف عن المعلومات لطرف ثالث موافقة على البحث؟** علاوة على ذلك، فإن النتيجة في قضية Hoffa انحازت إلى الإجابة الصحيحة: طالما أن الشخص يعرف أنه يكشف عن معلومات لطرف ثالث، فإن اختياره للقيام بذلك طوعي والموافقة صالحة. وحقيقة أن الشخص تبين أنه عميل سري لا صلة لها بما إذا كانت الموافقة صحيحة، لأن هذا التمثيل هو مجرد احتيال في الإغراء وليس احتيالا في الواقع[122]. والشخص الذي يكشف عن علم معلومات لطرف ثالث قد يخدع بشأن ما سيفعله الطرف الثالث بالمعلومات. لكن الخداع فيما يتعلق بالدافع أو التصميم لا يبطل الموافقة[123].

كيف خرجت المحكمة العليا عن مسارها؟ وكان المنعطف الحاسم هو قضية وايت ضد الولايات المتحدة. وايت[124]، وأول قضية طرف ثالث تتبع قضية (كاتز) Katz. وفي هذه الحالة، حاول القاضي وايت ملاءمة عقيدة الطرف الثالث في التعديل الرابع للمحكمة بعد (كاتز) Katz، لكنه ببساطة اختار الشق العقائدي الخاطئ. وبدلا من تأسيس المبدأ على مبادئ الموافقة، استنتج أن استخدام عميل سري لا ينتهك توقعا معقولا للخصوصية. الفرق بين الاثنين دقيق: إذا كان سلوك الحكومة لا ينتهك توقعا معقولا للخصوصية، فهو ليس تفتيشا[125]، وفي حين أنه إذا انتهك توقعا معقولا للخصوصية بموجب الموافقة، فهو بحث ولكنه بحث معقول دستوريا[126]. وفي الوقت نفسه، يغطي الاثنان أرضية متميزة من الناحية المفاهيمية. ويركز التوقع المعقول للتحقيق في الخصوصية على ما إذا كان سلوك الحكومة قد اقتحم المناطق المحمية دستوريا[127]، في حين أن الموافقة تسأل عما إذا كانت قد فعلت ذلك بإذن[128].

تبنت القضايا اللاحقة إطار عمل القاضي وايت دون تمحيص، وأنشأت فقه الطرف الثالث كتطبيق لاختبار قضية (كاتس)[129]. ولكن هذا الاساس العقائدي لا يصلح أبدا. إن تقاسم المساحة مع الآخرين لا يلغي حماية التعديل الرابع: تحتاج الشرطة إلى أذن warrant لدخول منزل مشترك بقدر ما تحتاج إلى منزل غير مشترك[130]. فإذا كان شخصان يتشاركان منزلا أو مكتبا، فإنهما لا يزالان يحتفظان بتوقع دستوري معقول للخصوصية هناك[131]. وتوفر مشاركة المساحة للساكن المشترك سلطة مشتركة للسماح بموافقته[132]، ولكنه لا يتخلى عن كل حماية التعديل الرابع. وبالمثل، فإن مبدأ الطرف الثالث يفهم بشكل أفضل على أنه مبدأ

---

[122] Id.
[123] See Rollin M. Perkins & Ronald N. Boyce, Criminal Law 1079 (3d ed. 1982). Perkins and Boyce note: The general rule is that if deception causes a misunderstanding as to the fact itself (fraud in the factum) there is no legally-recognized consent because what happened is not that for which consent was given; whereas consent induced by fraud is as effective as any other consent . . . if the deception relates not to the thing done but merely to some collateral matter (fraud in the inducement). Id.
[124] United States v. White, See id. at 1075–84. 401 U.S. 745 (1971).
[125] Smith v. Maryland, 442 U.S. 735, 740 (1979).
[126] See Georgia v. Randolph, 547 U.S. 103, 114–15 (2006).
[127] See Kyllo v. United States, 533 U.S. 27, 31 (2001) (citing Silverman v. United States, 365 U.S. 505, 510–12 (1961)).
[128] See Randolph, 547 U.S. at 114–15.
[129] See supra Section II.B.
[130] See Mancusi v. DeForte, 392 U.S. 364 (1968) (holding that a person retains a reasonable expectation of privacy in a shared office).
[131] Id. at 369–70.
[132] See United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (noting that "common authority" over spaces or property gives co-inhabitants the right to permit inspections of their own accord).

الفضاء المشترك. من خلال الكشف عن المعلومات عن قصد لطرف ثالث، ويوافق الفرد على سيطرة شخص آخر عليها. يبدو المذهب في الموافقة، وليس توقعات معقولة للخصوصية، ويتناسب مع بقية قانون التعديل الرابع عندما يفهم ذلك[133].

والأهم من ذلك، في حين أن هذه النقطة تضيق نطاق النقد العقائدي scope of the doctrinal critique، إلا أنها لا تلغيه تماما. على وجه الخصوص، ولا تتناول قضايا مثل ميلر حيث تجبر الحكومة طرفا ثالثا على الكشف عن السجلات بعد أن يكشف المشتبه به طواعية عن السجل للطرف الثالث. إذ وافق المشتبه به على وصول طرف ثالث في مثل هذه الحالات، لكن لم يوافق هو ولا الطرف الثالث على وصول الحكومة اللاحق. هذه نقطة عادلة. لكنني أعتقد أنه أيضا ضيق، حيث يصبح مبدأ الطرف الثالث في هذه المرحلة مجرد تطبيق للقاعدة العامة التي تنص على أن التعديل الرابع لا ينظم مذكرات الاستدعاء للإدلاء بشهادته[134]. ويمكن إجبار أي شاهد على الإدلاء بشهادته compelled to testify حول ما يعرفه وما رآه دون إشراف التعديل الرابع[135]، ومبدأ الطرف الثالث يمتنع فقط عن اقتطاع استثناء لهذه القاعدة للإفشاء السري لأطراف ثالثة.

B. بدائل لحمايات التعديل الرابع لمنع التحرش - حالة العملاء السريين

B. Alternatives to Fourth Amendment Protections to Prevent Harassment—The Case of Secret Agents

إن الانتقاد الرئيسي الثاني لفقه الطرف الثالث هو أنه يمنح الشرطة الكثير من السلطة[136]. وبحيث يسمح المبدأ للمسؤولين الحكوميين بإرسال جواسيس، واستخدام المخبرين، والحصول على السجلات المصرفية، وتسجيل الأرقام المطلوبة، والحصول على سجلات الفواتير لأشخاص أبرياء تماما دون أي سبب أو أمر من المحكمة. ووفقا للنقاد، فإن منح الحكومة هذا القدر من السلطة لا يتفق مع مجتمع حر ومفتوح. وخطر إساءة الاستخدام والمضايقة كبير جدا[137].

والمشكلة في هذه الحجة هي أنها تفترض أن التعديل الرابع هو اللعبة الوحيدة في المدينة. وفي الحقيقة، توجد مجموعة واسعة من الأدوات لمعالجة مضايقات الشرطة لمعلومات الطرف الثالث خارج التعديل الرابع. وتحل هذه الأدوات محل حماية التعديل الرابع، حيث تحظر أو تحد من الوصول إلى أدلة الطرف الثالث في أماكن محددة قد تكون عرضة لسوء الاستخدام. في حالة العملاء السريين، يستخدم النظام القانوني legal system قانون اعداد الفخ entrapment law، وفقه الماسايا Massiah doctrine ، والتعديل الأول، واللوائح الداخلية للحد من استخدام الحكومة للعملاء السريين. لكي نكون واضحين، هناك مجال كبير للنقاش

[133] Notably, Professor Colb has argued that the Supreme Court's "knowing exposure" cases should be reanalysed under consent principles. See Colb, supra note 67, at 123. However, Professor Colb does not focus this insight on the third-party doctrine cases specifically. Further, she does not suggest that the consent doctrine might help justify the existing third-party doctrine cases.
[134] United States v. Dionisio, 410 U.S. 1, 9 (1973).
[135] See id. at 10.
[136] See supra Section II.B.2.
[137] See supra Section II.B.2.

حول كفاية هذه البدائل لحماية التعديل الرابع. شرط الأمر هو دواء قوي، وبعض البدائل غير الدستورية متواضعة بالمقارنة comparison.

تم تصميم معظمها لردع التحقيقات بسوء نية بدلا من منع الحكومة من الوصول إلى المعلومات تماما، وقد يختلف المراقبون حول المذاهب التي تنجح أو تفشل. لكن هذا لا ينبغي أن يحجب النقطة الأعمق: حماية التعديل الرابع ليست سوى أداة واحدة من بين عدة أدوات لمعالجة مضايقات الشرطة. لا يعني غياب حماية التعديل الرابع أن ممارسات الشرطة غير منظمة. بدلا من ذلك، يعني التحول من التنظيم من خلال شرط ضمان سبب محتمل إلى التنظيم من خلال الامتيازات، ومبدأ الفخ، والتعديل السادس، والتعديل الأول، والقوانين، وغيرها من أشكال حماية الطرف الثالث.

باختصار، يعاني النقاد من قصر النظر الدستوري. بينما يركزون على فشل التعديل الرابع في وقف مضايقات الحكومة والحد من سلطة الدولة، فإنهم يميلون إلى التغاضي عن البدائل التي تعالج بالفعل نفس المخاوف من خلال وسائل أخرى. إذا تم تصوره بشكل صحيح، فإن الاختيار ليس بين حماية التعديل الرابع أو لا شيء، بل بين التنظيم من قبل مجموعة متنوعة من المذاهب أو تلك المجموعة المتنوعة من المذاهب بالإضافة إلى الحماية الإضافية للتعديل الرابع. ونتيجة لهذا فإن المنتقدين يبالغون في تقدير درجة سلطة الحكومة التي تسمح بها عقيدة الطرف الثالث.

يمكننا أن نبدأ بالنظر في كيفية محاولة القانون خارج التعديل الرابع تنظيم العملاء السريين. على الرغم من أن التعديل الرابع لا ينظم استخدام العملاء السريين[138]، إلا أن أربع مجموعات أخرى من القوانين تساعد في سد الفجوة: قانون الفخاخ. عقيدة ماسيا. التعديل الأول؛ ولوائح الوكالة الداخلية. جميع مجموعات القوانين الأربعة تردع انتهاكات العملاء السريين. وهي تحظر استخدام العملاء السريين في بعض الحالات وتضمن عدم استخدامهم إلا بطرق محدودة نسبيا في حالات أخرى.

1. قانون اعداد الفخ

1. Entrapment Law

يوفر قانون الفخ البديل الأول لتنظيم التعديل الرابع للعملاء السريين. الفخ هو مبدأ تم إنشاؤه قضائيا[139]، ومعترف به بموجب القانون في بعض الولايات[140]، ينظم كيفية استخدام الشرطة للعملاء السريين. على الرغم من وجود عدة أشكال من قانون الفخاخ، فإن الغرض الشامل من العقيدة هو فرض شرط ممارسات الشرطة المعقولة في استخدام العملاء السريين. وإذا استهدفت الشرطة شخصا بريئا، لم يظهر أي استعداد لارتكاب جريمة، لا يمكن للضابط السري أن يحث المستهدف على ارتكاب جريمة[141].

يحدث "الإغراء Inducement" عندما يضغط العميل السري على المشتبه به لارتكاب الجريمة، إما عن طريق إزعاجه أو تشجيعه على ارتكاب الجريمة بطريقة محسوبة لإقناع المشتبه به بناء على شخصيته[142].

[138] See supra Section I.A.1.
[139] See 2 Wayne La Fave et al., Criminal Procedure § 5.1(b) (3d ed. 2007).
[140] Id, See, e.g., Sherman v. United States, 356 U.S. 369 (1958).
[141] See, e.g., Sherman v. United States, 356 U.S. 369 (1958).
[142] Id.

والانتصاف هو الدفاع الإيجابي عن الملاحقة القضائية وليس قمع الأدلة، مما يعني أن معقولية سلوك الحكومة يتم تقييمها من قبل هيئة محلفين بدلا من قاض.

ان قانون اعداد الفخ Entrapment law يفعل مباشرة ما يريد منتقدو فقه الطرف الثالث القيام به بشكل غير مباشر: فهو ينظم ممارسات إنفاذ القانون المسيئة التي تستهدف المتهمين الأبرياء الذين لا يشتبه في ارتكابهم جريمة بالفعل. إن الشاغل الأساسي الذي يحرك قانون الفخ هو إلى حد كبير نفس الاهتمام الذي يحرك النقد الوظيفي لعقيدة الطرف الثالث: "السؤال الحاسم ... هو ما إذا كان سلوك الشرطة الذي تم الكشف عنه في حالة معينة أقل من المعايير. . . من أجل الاستخدام السليم للسلطة الحكومية"[143]. ولكن بدلا من تنظيم استخدام التحقيقات السرية مسبقا، يحظر قانون الفخاخ إساءة استخدامها في الممارسة العملية بأثر رجعي. بدلا من تنظيم متى يمكن استخدام العملاء السريين، فإنه ينظم كيفية استخدامها. تراقب مبادئ قانون الفخ سلوك الحكومة، مما يمنح هيئة المحلفين أساسا لتبرئة المدعى عليه إذا زرعت الحكومة فكرة الجريمة في ذهن المشتبه به.

إذا كان التعديل الرابع ينظم العملاء السريين، فلن يكون قانون الفخ ضروريا. في مثل هذا العالم، لن تستخدم الحكومة عملاء سريين إلا عندما يكون لديها سبب محتمل بأن المشتبه به سيكشف عن أدلة على جريمة، وأن الأدلة ستثبت الاستعداد لهزيمة دفاع الفخ[144]. لقد تطور قانون الفخ كمنتج لعقيدة الطرف الثالث. تم إنشاؤه من قبل المحاكم لسد الثغرات التي يتركها مبدأ الطرف الثالث مفتوحة.

2. فقه قضية مسايا

2. The Massiah Doctrine

البديل الثاني للائحة التعديل الرابع للعملاء السريين هو مبدأ قضية ماسيا. في قضية (ماسايا) ضد الولايات المتحدة[145]، ورأت المحكمة العليا أنه لا يمكن لعميل حكومي استجواب شخص متهم بارتكاب جريمة[146]. وتم توجيه الاتهام إلى (ماسايا) بتهم تتعلق بالمخدرات، وتم توكيل محام، وتم إطلاق سراحه بكفالة. التقى (ماسايا) لاحقا بشريكه في التآمر كولسون Colson، وناقش جرائم المخدرات التي ارتكبها مع كولسون عندما كان في سيارة كولسون[147]. دون علم (ماسايا) ، انقلب كولسون وكان يعمل كمخبر للحكومة. قام العملاء بالتنصت على سيارة كولسون ووجهوا كولسون لمناقشة جرائمه مع ماسيا. استمع عميل يدعى

[143] See, e.g., Sherman v. United States, 356 U.S. 369 (1958).
[144] United States v. Gendron, 18 F.3d 955, 961–62 (1st Cir. 1994). Examples listed by then Judge Breyer in Gendron include cases in which the secret agent (1) used intimidation and threats against a defendant's family; (2) called every day, began threatening the defendant, and was belligerent; (3) engaged in forceful solicitation and dogged insistence until defendant capitulated; (4) played upon defendant's sympathy for informant's common narcotics experience and withdrawal symptoms; (5) played upon sentiment of one former war buddy for another to get liquor (during prohibition); (6) used repeated suggestions which succeeded only when defendant had lost his job and needed money for his family's food and rent; and (7) told defendant that she (the agent) was suicidal and in desperate need of money.
[145] Sherman, 356 U.S. at 382 (Frankfurter, J., concurring).
[146] If the government cannot use a secret agent without probable cause to believe that the agent will uncover evidence of crime from the target, presumably that means that the government has prior evidence that the target is predisposed to engage in criminal activity.
[147] 377 U.S. 201 (1964).

مورفي Murphy إلى المحادثة وسمع تصريحات (ماسايا) التي تجرمه[148]. وفي المحاكمة، أدلى مورفي بشهادته حول ما سمعه بشأن اعتراض ماسيا. عندما وصلت قضية (ماسايا) إلى المحكمة العليا، جادل (ماسايا) بأن المراقبة السرية انتهكت التعديلات الرابع والخامس والسادس[149].

وقضت المحكمة العليا بأن هذا الاستخدام لعميل سري قد انتهك حقوق (ماسايا) في التعديل السادس[150]. أولا، رأت المحكمة لأول مرة أن الشخص الذي تم اتهامه ويمثله محام له الحق في عدم استجوابه من قبل المخبر بعيدا عن حضور محاميه[151]. ثانيا، ورأت المحكمة أن حقيقة أن "المرشد agent" كان مخبرا سريا لا فرق بينهما[152]. وفي الواقع، حقيقة أن (ماسايا) قد استجوب من قبل مخبر سري بدلا من ضابط شرطة يرتدي الزي الرسمي جعل انتهاك حقوقه أكثر فظاعة: "تم فرض ماسيا بشكل أكثر جدية على... لأنه لم يكن يعرف حتى أنه يخضع للاستجواب من قبل عميل حكومي" [153].

ينظم مبدأ Massiah استخدام أطراف ثالثة في الطرف الآخر من عملية التحقيق من قانون اعداد الفخ entrapment law. حيث يهتم قانون اعداد الفخ بكيفية تعامل الحكومة مع المشتبه بهم suspects في الواجهة الأمامية للتحقيقات: فلا يمكن للحكومة استخدام أطراف ثالثة لخلق جريمة لم تكن لتحدث لولا ذلك. ويهتم فقه (ماسايا) بكيفية تعامل الحكومة مع المشتبه بهم قرب نهاية العملية: في ظل (ماسايا)، لا يمكن للحكومة استخدام عملاء سريين للحصول على معلومات حول الجريمة من هدف تم اتهامه بالفعل. وفي حين أن التعديل الرابع يسمح باستخدام العملاء السريين عموما، فإن عقيدة (ماسايا) ترسم إحدى النتائج التي يحتمل أن تكون مسيئة لهذه القاعدة من خلال حظر هذه الممارسة بعد أن يمثل الشخص محام[154].

3. التعديل الاول

3. The First Amendment

قد يفرض التعديل الأول أيضا قيودا على استخدام العمليات السرية undercover operations. بشكل عام، يتورط التعديل الأول عندما يتسلل المحققون الحكوميون إلى الجماعات التي تشارك في أنشطة التعديل الأول دون سبب حسن النية good faith reason للقيام بذلك[155]. ويعالج اختبار حسن النية هذا نتيجة واحدة يخشى منتقدو عقيدة الطرف الثالث أن التعديل الرابع يسمح بها: التحقيقات المصممة لاستهداف الأفراد الذين يمارسون حقوقهم في التعديل الأول.

---

[148] Id. at 207 (“[W]e hold . . . that the defendant’s own incriminating statements, obtained by federal agents under the circumstances here disclosed, could not constitutionally be used by the prosecution as evidence against him at his trial.”).
[149] Id. at 202–03.
[150] Id.
[151] Id. at 203–04.
[152] Id. at 205–06.
[153] : “ ‘Massiah was more seriously imposed upon . . . because he did not even know that he was under interrogation by a government agent.’ ” Id. at 207.
[154] Id. at 206.
[155]

تقدم قضية Mayer [156] مثالا حديثا. فقد تسلل عميل سري لمكتب التحقيقات الفيدرالي إلى جمعية حب الرجل/الفتى في أمريكا الشمالية (“North American Man/Boy Love Association (”NAMBLA وهي مجموعة ادعت أنها "منظمة سياسية وحقوقية وتعليمية" تعارض قوانين سن الرضا[157]. وبعد أن أصبح عضوا نشطا في المجموعة، واجه العميل السري عدة مناقشات حول نشاط غير قانوني. أعرب أحد أعضاء المجموعة يدعى (ماير) عن إحباطه من أن (”NAMBLA“) استمرت في التظاهر بمحاولة تغيير المجتمع بينما في الواقع أراد أعضاؤها السفر فقط لمقابلة الأولاد"[158]. ثم رتب العميل السري رحلة لأعضاء NAMBLA لمقابلة الأولاد، واشترك (ماير) للذهاب في الرحلة. عندما ألقي القبض على (ماير) لسفره في التجارة بين الولايات بقصد الانخراط في أنشطة جنسية غير قانونية، ادعى أن تسلل الحكومة إلى (”NAMBLA“) ينتهك التعديل الأول.

ولقد أوضحت الدائرة التاسعة أن استخدام عميل سري للتسلل إلى مجموعة ذات صلة بالتعديل الأول لا يسمح به إلا عندما يكون "مبررا لغرض مشروع لإنفاذ القانون يفوق أي ضرر يلحق بمصالح التعديل الأول"[159]. ولقد وجدت المحكمة أن هذا الشرط قد تم الوفاء به، في ظل هذه الظروف، من خلال تقارير عن نشاط غير قانوني تلقته الشرطة فيما يتعلق بأعضاء مجموعة (”NAMBLA“) بالنظر إلى الحقائق، فإن "مصالح الحكومة في متابعة أهداف إنفاذ القانون المشروعة تفوق أي ضرر لمصالح التعديل الأول"[160]. فلو كان التحقيق السري يفتقر إلى غرض مشروع للسلطات legitimate law enforcement purpose، أو تم إجراؤه لتقليص حريات undertaken to abridge التعديل الأول، لكان التحقيق قد انتهك التعديل الأول على الرغم من أنه لم يورط التعديل الرابع.

4. اللوائح الداخلية للوكالة

4. Internal Agency Regulations

توفر اللوائح الداخلية للوكالة أداة رابعة للحد من استخدام العملاء السريين. اذ على المستوى الفيدرالي، على سبيل المثال، أصدرت وزارة العدل المبادئ التوجيهية للمدعي العام بشأن العمليات السرية لمكتب التحقيقات الفيدرالي[161]. حيث تتطلب المبادئ التوجيهية من الوكيل الخاص المسؤول عن كل مكتب من مكاتب مكتب التحقيقات الفيدرالي الموافقة المسبقة على كل تحقيق سري لمكتب التحقيقات الفيدرالي بناء على قرار مكتوب، مدعوم بحقائق محددة، بأن العملية المقترحة ستكون فعالة وستجرى بطريقة تداخلية بالحد

[156] United States v. Mayer، 503 F.3d 740 (9th Cir. 2007).
[157] the North American Man/Boy Love Association (“NAMBLA”): a group that claimed to be “a political, civil rights and educational organization’ ” opposed to age-of-consent laws. Id. at 745.
[158] Mayer expressed in frustration that “NAMBLA kept up pretenses of trying to change society when in fact its members only wanted to travel to meet boys.” Id. at 747.
[159] “justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests.” Id. at 753.
[160] the government’s “interests in pursuing legitimate law enforcement objectives outweighed any harm to First Amendment interests.” Id.
[161] the Justice Department has promulgated the Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations. John Ashcroft, Att’y Gen., The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations (2002), available at http://www.usdoj.gov/olp/fbiundercover.pdf.

الأدنى[162]. ويمكن الموافقة على العمليات السرية لمدة تصل إلى ستة أشهر وتجديدها لفترة ستة أشهر أخرى[163]. ولا يمكن أن تنطوي عادة على نفقات تزيد عن 50000 دولار[164].

وتتضمن المبادئ التوجيهية قواعد خاصة للتحقيقات السرية الحساسة sensitive undercover investigations بشكل خاص. يجب أن يوافق مقر مكتب التحقيقات الفيدرالي مسبقا على التحقيقات في المنظمات السياسية political organizations أو الجماعات الدينية religious groups أو وسائل الإعلام news media أو المسؤولين العموميين public officials[165]. حيث تجتمع لجنة مراجعة العمليات السرية الجنائية المكونة من مسؤولي مكتب التحقيقات الفيدرالي ووزارة العدل لمراجعة هذه الطلبات، ويجب أن تتوصل إلى توافق في الآراء بشأن مدى ملاءمة كل طلب[166]. فإذا أوصت اللجنة بالموافقة على طلب ما، فيجب أن تتضمن بيانا عن سبب استحقاق العملية للموافقة في ضوء الطبيعة الحساسة لمثل هذه الطلبات التحقيقات[167]. فقد أصدرت وزارة العدل مبادئ توجيهية مماثلة تقريبا لاستخدام المخبرين السريين[168]. فمثل القيود التي يفرضها قانون اعداد الفخ، وفق فضية ماسيا، والتعديل الأول، تحاول قواعد الوكالة هذه منع استخدام العملاء السريين بسوء نية bad faith أو في سياقات مسيئة abusive contexts.

C. بدائل لحماية التعديل الرابع في قضايا سجلات الأعمال

C. Substitutes for Fourth Amendment Protection in Business Record Cases

مثلما تنظم العديد من الأدوات القانونية legal tools استخدام العملاء السريين، هناك العديد من البدائل لحماية التعديل الرابع للسجلات التجارية. الأدوات القانونية الثلاث السائدة هي الحماية التشريعية statutory protections وامتيازات القانون العام common law privileges وحقوق الأطراف الثالثة نفسها rights of the third parties. وتنظم هذه المذاهب وصول الحكومة إلى السجلات التجارية خارج التعديل الرابع، مما يردع أنواع الانتهاكات التي يخشى النقاد من حدوثها بموجب مبدأ الطرف الثالث. وفي بعض الحالات، تتطلب هذه الأدوات أوامر من المحكمة court orders أو سبب خاص special cause للوصول إلى سجلات الطرف الثالث؛ وفي حالات أخرى، يتم منع الوصول إلى سجلات الجهات الخارجية تماما. وهذه المذاهب مجتمعة تحد إلى حد كبير من التهديد الذي يشكله فقه الطرف الثالث على الحريات المدنية. ومرة أخرى، يمكن أن تختلف العقول المعقولة حول ما إذا كانت تفعل ما يكفي في حالات محددة. لكن هذه المذاهب تساعد في معالجة التهديد للخصوصية والحقوق الفردية الذي يلاحظه النقاد عند النظر إلى عقيدة الطرف الثالث بمعزل عن غيرها.

---

[162] Id. at 3–4.
[163] Id. at 4.
[164] Id.
[165] Id. at 6.
[166] Id. at 8.
[167]
[168] Id. at 8.

1. الحماية التشريعية

1. Statutory Protections

ان البدائل الأكثر وضوحا للتنظيم الدستوري للوصول إلى سجلات الأعمال هي الحماية التشريعية. يمكن لتشريعات الخصوصية القانونية Statutory privacy laws أن تفرض شرطا بأمر من المحكمة على جمع الأدلة الحكومية حتى لو لم يفعل التعديل الرابع. ويمكن أن تردع النتيجة مضايقة الأبرياء من خلال إدخال الإشراف القضائي على التحقيقات ومطالبة المسؤولين فعليا بإثبات مصلحة حكومية مشروعة في المعلومات المطلوبة.

على سبيل المثال، ردا على قضية (سميث) [169] Smith، سن الكونجرس قانون سجل القلم والفخ وأجهزة التتبع، المقنن في 18 USC 3121-3127.[170] فقد رأى (سميث) أن التعديل الرابع لا يحد من استخدام أجهزة تسجيل القلم لتحديد الأرقام التي يتم الاتصال بها من الهاتف[171]. ومع ذلك، فإن قانون سجل القلم يجرم تثبيت سجل القلم دون أمر من المحكمة، مع مراعاة بعض الاستثناءات. والحصول على أمر من المحكمة court order أمر سهل للغاية بموجب النظام التشريع: يحتاج المحققون فقط إلى التصديق على أن "المعلومات التي من المحتمل الحصول عليها ... ذات صلة بتحقيق جنائي جار"[172]. ولكن هذا لا يزال يفرض اختبارا لحسن النية: يتطلب القانون تحقيقا فعليا جاريا واعتقادا بحسن نية في احتمال أن تكون الأدلة التي سيتم الحصول عليها ذات صلة بهذا التحقيق.

وبالمثل، ردا على (ميلر)[173]، سن الكونغرس قانون الحق في الخصوصية المالية RFPA [174]. حيث يستجيب RFPA لميلر من خلال تقييد وصول الحكومة إلى "المعلومات الواردة في السجلات المالية لأي عميل من مؤسسة مالية"[175] حيث التعديل الرابع، وبفضل (ميلر)، لا يفعل ذلك. وبموجب قانون RFPA، لا يمكن للحكومة الحصول على مثل هذه السجلات المالية RFPA بأمر استدعاء subpoena إلا إذا كان لدى الحكومة "سبب للاعتقاد بأن السجلات المطلوبة ذات صلة بتحقيق شرعي لدى السلطات وقدمت الحكومة أولا للمشتبه به إشعارا مسبقا prior notice بالإجراء المخطط له الذي يمنحه فرصة للتحرك لإلغاء أمر الاستدعاء move to quash the subpoena[176].

في بعض الحالات، تم سن الحماية القانونية لسجلات الطرف الثالث حتى في غياب قرارات المحكمة. على سبيل المثال، يحمي قانون إخضاع التأمين الصحي لقابلية النقل والمساءلة السجلات الطبية HIPAA[177] حيث يقيد قانون حماية الخصوصية وصول الحكومة إلى سجلات الطرف الثالث التي تحتفظ بها منظمات

---

[169] the Pen Register and Trap and Trace Devices Statute. See Department of Justice Guidelines Regarding the Use of Confidential Informants (Jan. 8, 2001), http://www.usdoj.gov/ag/readingroom/ciguidelines.htm.
[170] Smith v. Maryland, 442 U.S. 735 (1979). 18 U.S.C. §§ 3121–3127 (2000 & Supp. V 2005).
[171] Smith, 442 U.S. at 743.
[172] "the information likely to be obtained . . . is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a) (2000).
[173] United States v. Miller, 425 U.S. 435 (1976).
[174] the Right to Financial Privacy Act ("RFPA"). 12 U.S.C. §§ 3401–3422 (2006).
[175] "the information contained in the financial records of any customer from a financial institution". 12 U.S.C. § 3402.
[176] "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry" 12 U.S.C. § 3407.
[177] Health Insurance Portability and Accountability Act ("HIPAA")

جمع الأخبار[178]؛ حيث يوفر قانون حماية خصوصية الفيديو حماية خصوصية خاصة لسجلات تأجير الفيديو[179]؛ ويقيد قانون الاتصالات المخزنة الوصول إلى سجلات حساب البريد الإلكتروني؛[180] ويقيد قانون الكابل الوصول إلى سجلات حساب الكابل[181]. حيث تفرض جميع هذه القوانين تلك القيود المفروضة على الوصول إلى السجلات التي يتركها فقه الطرف الثالث دون حماية بموجب التعديل الرابع.

في العديد من هذه الحالات (وليس كلها)، توفر قوانين الخصوصية التشريعية حماية أقل مما يبرره معيار التعديل الرابع المماثل لسبب محتمل probable cause warrant [182]. ولكن هذا أمر جيد وليس سيئا. حقيقة أن المعايير منخفضة تمنع الالتفاف النهائي حول توازن قواعد التعديل الرابع التي يمكن أن تسمح بها الاستعانة بمصادر خارجية. وفي الوقت نفسه، فإن المعايير كبيرة بما يكفي لجعلها غير المرجح أن تستخدم الشرطة لسلطات التحقيق فقط لمضايقة المشتبه بهم الأبرياء.

في حالة السجلات المالية financial records، يمكن للمشتبه به التحرك لإلغاء أمر الاستدعاء move to quash the subpoena، والذي من شأنه أن يوفر للمحكمة علنية court audience للاستماع إلى شكواه من تجاوز الحكومة. وفي حالة سجلات القلم، يجب على الحكومة أولا الذهاب إلى قاض والسعي للحصول على أمر، والتصديق تحت القسم على وجود تحقيق مستمر وأن المعلومات التي تم جمعها من المرجح أن تكون ذات صلة. هذه المعايير الوسيطة تردع الانتهاكات غير المشروعة بينما تسمح بإجراء تحقيقات مشروعة. إنهم يصطدمون بأرضية مشتركة غير ممكنة بموجب التعديل الرابع.

2. امتيازات القانون العام/ السوابق

2. Common Law Privileges

توفر امتيازات القانون العام أداة ثانية لتنظيم الوصول إلى السجلات التجارية. فعندما يكون للمشتبه به علاقة مميزة مع طرف ثالث، لا يمكن للحكومة الوصول إلى سجلات الطرف الثالث. ومن الناحية العملية، يتفوق الامتياز على فقه الطرف الثالث. حيث إنه يجبر الحكومة على اتباع نهج عدم التدخل في ما قد يكون معلومات محرجة للغاية very embarrassing information أو أدلة مهمة على النشاط الإجرامي important evidence of criminal activity.

المثال الأكثر وضوحا للامتياز الذي يتفوق على مبدأ الطرف الثالث هو امتياز المحامي والموكل. في النظام الفيدرالي، يتم الاعتراف بالامتيازات بموجب قاعدة الإثبات الفيدرالية: "امتياز الشاهد privilege of a witness [أو] الشخص ... المحكوم بمبادئ القانون العام كما قد تفسرها محاكم الولايات المتحدة في ضوء العقل والخبرة "[183]. بموجب امتياز العلاقة بين المحامي وموكله attorney-client privilege، حيث "يتمتع بامتياز الكشف السري من قبل موكله إلى محام من أجل الحصول على مساعدة قانونية"[184]. تشجع

[178] 45 C.F.R. § 164.512(f)(1)(ii)(A) (2007) (permitting disclosure of medical records pursuant to "[a] court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer").
[179] 18 U.S.C. § 2710.
[180] 18 U.S.C. § 2703(c) (Supp. V 2005).
[181] 47 U.S.C. § 551(h).
[182] 42 U.S.C. § 2000aa (2000).
[183] 18 U.S.C. § 2710
[184] 18 U.S.C. § 2703(c) (Supp. V 2005).

هذه القاعدة "الاتصال الكامل والصريح بين المحامين وموكليهم، ومن ثم تعزز المصالح العامة الأوسع نطاقا في احترام القانون وإقامة العدل"[185]. بحيث يجب رفض الأدلة التي يتم جمعها حين انتهاك للامتياز.

امتياز المحامي وموكله ليس الامتياز الوحيد المعترف به من قبل المحاكم الفيدرالية. اعترفت المحكمة العليا بامتياز المعالج النفسي والمريض في قضية جافي ضد ريدموند[186]. وعلى الرغم من أن المحكمة العليا لم تعالج هذه القضية، فقد اعترفت المحاكم الفيدرالية الدنيا عموما بامتياز الكاهن التائب penitent priest privilege [187]. فكل هذه الامتيازات تتفوق فعليا على فقه الطرف الثالث في أماكن محددة حيث يكون الاستعانة بمصادر خارجية للجريمة غير مرجح بشكل خاص أو هناك احتياجات منافسة قوية تتجاوز جمع الأدلة. من غير المرجح أن يستخدم المشتبه به محاميه أو كاهنه أو معالجه النفسي لتسهيل جرائمه، ومن غير المرجح أن يكون المحامون المحترفون ورجال الدين وعلماء النفس على استعداد للمشاركة في تعزيز المخطط الإجرامي للعميل. وفي الوقت نفسه، هناك حاجة إلى الامتياز للسماح للأفراد بالاستفادة من مشورة محاميهم وكهنتهم ومعالجيهم. وفي هذه الظروف، يخفف الامتياز بشكل فعال من التهديد المحتمل لانتهاكات الحكومة التي تثيرها عقيدة الطرف الثالث.

3. حقوق الاطراف الثالثة

3. The Rights of Third Parties

ان الأداة الأخيرة لتنظيم وصول الحكومة إلى السجلات التجارية لأطراف ثالثة هي من خلال حقوق الأطراف الثالثة نفسها. وفي بعض الحالات، قد تكون الأطراف الثالثة التي لديها سجلات تجارية على استعداد للتعاون مع الشرطة. ومع ذلك، وفي العديد من السياقات، قد ترغب الأطراف الثالثة في تأكيد حقوق عملائها. اذ تعد حماية خصوصية العملاء أمرا جيدا للأعمال التجارية، وغالبا ما يكون لدى حاملي السجلات من الأطراف الثالثة حافز كبير لإبقاء الحكومة في مأزق. ومن الأمثلة المبكرة على ذلك موجز صديق المحكمة الشهير الذي قدمته شركات الهاتف في أول قضية تنصت على المكالمات الهاتفية للمحكمة العليا، (أولمستيد) ضد الولايات المتحدة[188].

حثت شركات الهاتف المحكمة العليا على الحكم بأن الحكومة لا يمكنها التنصت على خطوط الهاتف[189]. ومثل هذه القاعدة منطقية من الناحية التجارية لشركات الهاتف: فهي ستشجع العملاء على استخدام الهاتف وتمنع الحكومة من التدخل في شبكاتهم.

يوضح مثال أحدث كيف يمكن لمزودي الخدمات الخارجيين الحديثين modern third-party providers تأكيد حقوق العملاء على الرغم من مبدأ الطرف الثالث. ففي عام 2006، وفي خضم التقاضي المدني بشأن

---

[185] 47 U.S.C. § 551(h).
The major exception is the Cable Act, which allows disclosure of cable records only in very narrow circumstances. Id.
[186] Jaffee v. Redmond. 518 U.S. 1, 15 (1996).
[187] Cox v. Miller, 296 F.3d 89, 102 n.6 (2d Cir. 2002) (citing cases).
[188] 277 U.S. 438 (1928).
[189] Brief for Pacific Telephone & Telegraph Co. et al. as Amici Curiae Supporting Petitioners, Olmstead v. United States, 277 U.S. 438 (1928) (Nos. 493, 532, 533).

دستورية قانون حماية الأطفال على الإنترنت Child Online Protection Act، أصدرت وزارة العدل DOJ مذكرات استدعاء تأمر العديد من شركات محركات البحث بالكشف عن استفسارات المستخدمين لمدة شهرين[190]. ولقد ادعت وزارة العدل أنها بحاجة إلى هذه المعلومات لتحديد كيفية استخدام مستخدمي الإنترنت لمحركات البحث للحصول على المواد الإباحية، والتي يمكن أن تساعد بعد ذلك في تحديد فعالية فلاتر/ مرشحات الإنترنت Internet filters [191]. وعندما اعترضت Google على مذكرات الاستدعاء objected to the subpoenas، وافقت وزارة العدل على أمر استدعاء subpoena أضيق يسعى للحصول على مليون استعلام عشوائي وجميع عمليات البحث عن نافذة مدتها أسبوع واحد[192]. ثم واصلت Google الاعتراض، وتحركت لإلغاء مذكرات الاستدعاء على أساس أنها سعت للحصول على معلومات غير ذات صلة وأن الإنتاج سيكون عبئا لا داعي له. قدمت Google القضية بشكل إبداعي إلى حد ما، بحجة أن "احتمال فقدان ثقة المستخدم" كان "عبئا" على Google يجب أن يتطلب إلغاء مذكرات الاستدعاء[193].

لقد استخدم قاضي محكمة المقاطعة جيمس وير Judge Ware هذه المبادئ القانونية لصياغة أمر استدعاء ضيق يحمي مصالح الخصوصية لمستخدمي Google. وفقا لتعديل القاضي (وير) Judge Ware، فقد تطلب أمر الاستدعاء من Google إنشاء قاعدة بيانات تقدم اختيارا عشوائيا ل 50000 عنوان موقع ويب يمكن الوصول إليها من خلال محرك بحث Google [194]. ولقد أثار القاضي وير Judge sua sponte Ware مسألة مصالح الخصوصية لمستخدمي Google وليس مصالح الخصوصية في التعديل الرابع، ولنكون واضحين، ولكن مصالح الخصوصية الأكثر عمومية في الكشف عن المعلومات التي أرسلها المستخدمون إلى Google في استفساراتهم[195]. حيث لاحظ القاضي (وير) أنه يمكن أن تحتوي استعلامات البحث على معلومات شخصية، مستشهدا باستعلامات الغرور أو الاستعلامات citing vanity queries or queries عن المعلومات الجنسية الصريحة كأمثلة على الاستعلامات التي تثير مخاوف تتعلق بالخصوصية[196]. وقد صمم أمر استدعاء يسمح للحكومة بإجراء دراسة حول نتائج Google دون أن يؤدي ذلك إلى الكشف عن استفسارات الجهات الخارجية التي أجراها المستخدمون.

في عدد من القضايا، نجحت أطراف ثالثة أيضا في تأكيد مصالح التعديل الأول للمستخدمين استجابة لمذكرات الاستدعاء المسموح بها بموجب التعديل الرابع. وعلى سبيل المثال، في قضية Doe جادل (غونزاليس)[197]، مزود خدمة الإنترنت Internet Service Provider في ولاية كونيتيكت Connecticut بنجاح بأن التعديل الأول منحه الحق في الكشف عن خدمة خطاب الأمن القومي لمعلومات سجل الطرف الثالث. وفي قضية استدعاء حديثة أخرى، حكم قاض جزئي magistrate judge بأن اصدار امر احضار subpoena عن هيئة محلفين كبرى grand jury لسجلات الطرف الثالث لشراء الكتب انتهك التعديل الأول من خلال

[190] See Declan McCullagh, FAQ: What does the Google subpoena mean? CNET News, Jan. 20, 2006, http://news.cnet.com/2100-1029_3-6029042.html.
[191] Id.
[192] Gonzales v. Google, Inc., 234 F.R.D. 674, 683 (N.D. Cal. 2006).
[193] Id. at 688.
[194] Id. at 688.
[195] Id. at 687.
[196] Id
[197] Doe v. Gonzales, 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

إحداث تأثير مخيف محتمل على الشراء[198]. بالإضافة إلى ذلك، فرضت عدة محاكم قيودا بموجب التعديل الأول على مذكرات الاستدعاء لسجلات الطرف الثالث في السياق المدني[199].

أنا لا أزعم أن أصحاب السجلات التجارية من طرف ثالث سيؤكدون دائما هذه الحجج دفاعا عن عملائهم. في الواقع، تؤكد العناوين الأخيرة[200] كيفية مساعدة مزودي الاتصالات طواعية لوكالة الأمن القومي في جمع سجلات الطرف الثالث (ربما في انتهاك لقوانين الخصوصية القانونية)[201]أنه في بعض الأحيان يتعاون مزودو الطرف الثالث بشغف مع الحكومة. لكن النقطة أوسع. يمكن لأصحاب السجلات التجارية من الأطراف الثالثة التعرف على مزايا الكفاح من أجل حقوق الخصوصية لعملائهم حتى في غياب حماية التعديل الرابع. غالبا ما يخلق احتمال المقاومة من الفرق القانونية لأصحاب السجلات من الأطراف الثالثة رادعا كبيرا ضد تجاوز الحكومة حتى عندما لا تفعل عقيدة الطرف الثالث.

[198] In re Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 573 (W.D. Wis. 2007).
[199] See generally Daniel J. Solove, The First Amendment as Criminal Procedure, 82 N.Y.U. L. Rev. 112 (2007) (exploring the relationship between the First Amendment and criminal procedure).
(استكشاف العلاقة بين التعديل الأول والإجراءات الجنائية).
[200] See, e.g., Jason DeParle, Deal Close on Wiretap Law, a Top Democrat Tells CNN, N.Y. Times, Mar. 3, 2008, at A13. Of course, by the time this Article is published, this story will be "old news"!
[201] See generally Orin S. Kerr, Civil Liability and the NSA Call Records Program, http://www.orinkerr.com/2006/05/12/civil-liability-and-the-nsa-call-records-program/ (May 12, 2006, 17:00 EST).

خلاصة

Conclusion

وقد دعت هذه المادة إلى فهم جديد لمبدأ الطرف الثالث. يصوره منتقدو العقيدة على أنها خيار بين كل شيء أو لا شيء، بين حماية التعديل الرابع أو عدم الحماية على الإطلاق[202]. ومن وجهة نظرهم، فإن قضايا فقه الطرف الثالث "تسخر mockery من التعديل الرابع" [203]، تاركة فراغا دستوريا constitutional void غير منطقي illogical وغير متسق inconsistent مع مجتمع حر free society [204]. حيث اقترح هذا المقال أن هذا الرأي السائد على نطاق واسع لا يروي سوى نصف القصة. يخدم فقه الطرف الثالث دورين مهمين: منع تأثيرات الاستبدال substitution effects التي تزعج الحياد التكنولوجي technological neutrality لنص التعديل الرابع وزيادة وضوح قواعد التعديل الرابع. علاوة على ذلك، فإن آثار العقيدة أقل خطورة بكثير مما يميل النقاد إلى اقتراحه. هذا المبدأ ليس سوى أداة واحدة من بين العديد من الأدوات لمعالجة انتهاكات الأطراف الثالثة.

وباختصار، يجب أن تراعي تكاليف ومنافع مبدأ الطرف الثالث آثار الاستبدال. وعلى جانب التكلفة، لابد من تعويض المخاوف من السلطة الحكومية المفرطة بتأثيرات الإحلال substitution effects لمذاهب مثل الفخ entrapment، وامتيازات القانون العام، والحماية التشريعية، وفقه قضية ماسيا. وعلى جانب الفوائد، يجب على المحاكم النظر في كيفية تأثير الاستبدال لخدمات الطرف الثالث يمكن أن يخل بالتوازن التقليدي upset the traditional balance لقواعد التعديل الرابع. حيث إن التقدير الكامل لدور فقه الطرف الثالث يكشف أنها أكثر تعقيدا مما ادعى النقاد. هذا لا يعني أن كل تطبيق لهذا الفقه صحيح بلا منازع. وهناك مجال للخلاف في حالات محددة، لا سيما بالنظر إلى صعوبة تقييم التكاليف والفوائد التي ينطوي عليها الأمر. ولكن عندما يتم فهم الصورة بأكملها، فإن فقه الطرف الثالث له مكان مهم في نظام مناسب لقواعد الإجراءات الجنائية[205].

وعلى نطاق أوسع، يكشف دور فقه الطرف الثالث عن نقطة عمياء شائعة جدا common blind all-too spot بين فقهاء الإجراءات الجنائية criminal procedure scholars. غالبا ما ركز النقاد على سلطات الحكومة لمضايقة الأفراد الأبرياء، وبحثوا عن طرق يمكن للدستور من خلالها منع المضايقات harassment [206]. ولكن قضاة المحكمة العليا Justices of the Supreme Court لا يتمتعون بهذا الترف luxury. ويتعين على المحكمة أن تضع قواعد تنطبق على التحقيقات مع كل من الأبرياء والمذنبين في عالم لا تستطيع فيه الحكومة في كثير من الأحيان التمييز بين الاثنين في البداية. يجب أن ينظروا بشكل منهجي لإنشاء مجموعة من القواعد التي ستنطبق على كليهما.

ومن هذا المنظور، فإن شرط مذكرة التعديل الرابع هو دواء قوي strong medicine -وأحيانا قوي جدا too strong. صحيح أنه يردع الانتهاكات، لكنه يوقف أيضا التحقيقات المشروعة legitimate بحسن نية.

---

[202] See generally Orin S. Kerr, Civil Liability and the NSA Call Records Program, http://www.orinkerr.com/2006/05/12/civil-liability-and-the-nsa-call-records-program/ (May 12, 2006, 17:00 EST).
[203] See supra Section I.B.
[204] 1 LaFave, supra note 7, §2.7(b), at 736.
[205] See supra Section I.B.
[206] See supra notes 5–11 and accompanying text.

وفي المراحل الأولية من التحقيقات، يجب أن يكون لدى الشرطة أدوات لجمع الأدلة لتحديد ما إذا كان هناك سبب محتمل probable cause؛ يمكن بعد ذلك حفظ متطلبات الأمر للحد من الممارسات الأكثر توغلا مثل تفتيش المنازل والطرود searches of homes and packages.

في حين أن هذا يزيل التدقيق في التعديل الرابع من مجموعة من ممارسات الطرف الثالث، فإنه يميل إلى القيام بذلك عندما تكون الممارسات في الأساس معاملات - مسألة من فعل ماذا، وليس ما كان يفكر فيه شخص ما أو يقوله أو يشعر به. حيث يمكن لمصادر أخرى لقانون الخصوصية بعد ذلك سد الفجوة، وردع الممارسات المسيئة دون فرض عتبة عالية من متطلبات مذكرة التعديل الرابع. والنتيجة هي نظام من القواعد الإجرائية التي تحمي الأبرياء innocent وتسمح بالتحقيقات والملاحقات القضائية للمذنبين.

لسوء الحظ، فشلت المحكمة العليا فشلا ذريعا في توضيح هذه المبادئ. وعندما تواجه المحكمة وقائع قضايا محددة، تكون قد توصلت إلى نتائج أعتقد أنها صحيحة. ولكن من خلال تقديم القضية بشكل غير صحيح في التوقع المعقول لاختبار الخصوصية بدلا من قانون الموافقة/ الارادة consent law، فقد وضعت المحكمة نفسها في زاوية بلاغية rhetorical corner وتركت المبدأ غير مفسر إلى حد كبير. وتوحي أهمية سجلات الأطراف الثالثة في التكنولوجيات الجديدة والانتقادات المستمرة للسوابق القضائية للمحكمة بأن الوقت قد حان لكي تطور المحاكم والمعلقون على حد سواء فهما أكثر تطورا لمبدأ الطرف الثالث. يجب إعادة صياغة الفقه بدلا من طرحها جانبا.

إعداد :
فرج بشير برنوص
ماجستير قانون جنائي (فرع قانون الانترنت)
خبير محلف فى الجرائم الافتراضية 2017م

عنوان الرسالة:
أذن التفتيش الممتد وآثاره في الجرائم الافتراضية

(جزء من رسالتي لاستكمال متطلبات الإجازة العالية «الماجستير» في القانون الجنائي)

الموسومة:
التفتيش والضبط في الجرائم الافتراضية: دراسة تحليلية مقارنة

تاريخ المناقشة: 2012/01/21

المطلب الثاني

تنفيذ التفتيش

تمهيد وتقسيم /

ترتكز النظرية العامة للتفتيش في إطار جرائم العالم الافتراضي على أساس مهم وهو أولويات البحث عند القيام بالتفتيش، ذلك أنه يجب أن تكون هناك خطوات مدروسة ومرتبة بشكل منطقي وإلا فقد التفتيش قيمته القانونية وهذه الخطوات يجب أن تجرى حسب الترتيب التالي:

1-التفتيش والبحث في الخادم.

2-الانتقال إلى تفتيش مسار الإنترنت وحركة البيانات.

3-تفتيش حاسوب المتهم.

4-تفتيش حاسوب المجني عليه وهي حالة استثنائية تجرى في حالات ضيقة ومحددة وحسب ظروف كل واقعة (1). ومن هذا الترتيب المنطقي لهذه الخطوات يفهم منها أنه لا يجوز القيام بخطوة دون أن تسبقها الخطوة الأولى حسب الترتيب. ويجب أن يتم تدوين ذلك في محضر التفتيش إمكانية إجراء الخطوة أو صعوبة إجرائها وأسباب ذلك. وإذا لم يثبت ذلك في محضر إجراءات التفتيش كان الدليل المستمد منه باطلاً. ومع ذلك فإذا تم إجراء إحدى الخطوات وتم ضبط الدليل الرقمي وهو كاف لإقامة الدعوى الجنائية فلا داعي لاستكمال باقي الخطوات (2). ولأن التفتيش في إطار البحث عن الأدلة في الجرائم الافتراضية من المسائل ذات الأهمية البالغة ولذلك فإن أي تجاوز أو خطأ قد تنتهي به الدعوى الجنائية قبل أن تولد وهو ما يحمل سلطات التحقيق مسؤولية أكبر وأدق عند القيام بهذا الإجراء. وسوف نتعرض للخطوات السابقة بشيء من التفصيل لأهميتها عند إجراء التفتيش من خلال ما سنتناوله في **الفرع الاول/** تفتيش الخوادم والمضيفات وتفتيش مسار الإنترنت وحركة البيانات وتفتيش حاسوب الجاني وتفتيش حاسوب المجني عليه استثناءً وفي **الفرع الثاني** سأتناول التفتيش الرقمي.

1. مشروع المذكرة الايضاحية لمشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا (مقترح موسوعة التشريعات العربية – محمد ابوبكر بن يونس).
2. نفس المرجع السابق.

الفرع الاول

تفتيش الخوادم والحواسيب والشبكات

أولا: تفتيش الخوادم والمضيفات:

الأصل أن إذن التفتيش يجب أن يحدد مكان وزمان التفتيش للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات او حصول التحقيق بشأنها وهي الغاية من التفتيش (مادة 39 إجراءات جنائية ليبي), والالتزام بهذه القواعد هو شرط لصحة إجرائه لأن التفتيش هو إجراء من إجراءات التحقيق الخطيرة ومن الناحية العملية يجب أن يكون الشخص القائم بإجراء التفتيش من ذوي الخبرة في هذا المجال , وتحديد الأماكن والأشياء والمعدات المراد تفتيشها يتطلب معرفتها بدقة والعلم بها , وجزئية الأماكن من الأمور الصعب تحديدها في الجرائم الافتراضية.

ولكن ما هو المقصود بالخوادم والمضيفات؟ وهل هناك مسؤولية قانونية يتحملها الخادم أو المزود عن الجرائم المرتكبة عبره؟ وللإجابة عن ذلك نقول إن الخادم server هو عبارة عن جهاز حاسوب ذي مواصفات عالية جداً ونظام تشغيل خاص يقوم بتخزين البرامج والملفات التي تكون مادة المواقع الإلكترونية حتى يتمكن زوار هذه المواقع من تصفحها على الإنترنت وهي تنقسم إلى ثلاثة أنواع : خادم من فئة الحاسوب الشخصي pc وخادم من فئة محطات العملwork station وخادم من فئة الحاسبات الرئيسية mainframe وقد يطلق على الخادم اختصار ISP وقد عرفته المحاكم الأمريكية بالآتي (**إن الخادم أو الملقم server هو عبارة عن حاسوب computer يسمح بتزويد الخدمات للحواسيب الأخرى ، حيث يقوم باستضافة Hosts المواقع websites وتجميع وتنظيم البيانات المحصلة من المستخدمين ولكنه لا يقوم بإعداد نسخ من الملفات المتبادلة ذاتها**) (1) كذلك فإن عبارة الخادم أو المضيف والمزود تؤدي إلى نفس المعنى في أغلب الدراسات المطروحة ويطلق على الحواسيب المضيفة host computers وهي جميع الحواسيب المتصلة بالإنترنت أما المقصود بالاستضافة فهي عبارة عن مجموعة من الخوادم

1- د. عمر محمد بن يونس – أشهر المبادئ المتعلقة بالإنترنت في القضاء الامريكي – دار النهضة العربية – القاهرة – 2007م –ص348

المتصلة بعضها ببعض والتي تحتوي على محتوى المواقع (1) الذي يمكن لأجهزة الحاسوب الأخرى الوصول إليها عبر الإنترنت. فمزود الاستضافة هو خادم يؤدي وظيفة تخزين البيانات مع إمكانية تراسلها أو استردادها إن الأنشطة التي تشير إلى مزود الإنترنت مباشرة هي التزويد بالاتصال والتزويد بالدخول، إلا أن مسألة نشاط مزود الخدمة وتميزه عن نشاط المزود المعلوماتي ليست بالعملية السهلة إلا ان المشرع الأمريكي في قانون آداب الاتصالات لسنة 1996م. ميز بين المزود المعلوماتي عبر الإنترنت وبين مزود الدخول إلى الإنترنت وكذلك فعل المشرع المقارن من بعده (2).

أما مسؤولية الخادم أو مزود الخدمة عن الجرائم الافتراضية فإنه يلاحظ انقساماً في الفقه المقارن إلى اتجاهين / الأول بعض من الفقه العربي أو يمكن أن نطلق عليه المنهج العربي والذي أقر مبدأ مسؤولية الخادم وهذا الأخير يرى تطبيق مبدأ المسؤولية التقصيرية طبقاً لأحكام القانون المدني على حالة مسؤولية الخادم ويلاحظ أن بعضاً من الفقه الغربي أيد هذا المنهج العربي ومنها على سبيل المثال الفقه الألماني والإيطالي. وقد برز هذا الاتجاه المؤيد في مؤتمر بون الدولي 1997م. وقد استمد المؤتمر المذكور أغلب أفكاره ومقرراته من قرارات وزيرة العدل الأمريكية Jannet Renu في عهد حكومة الرئيس كلينتون والذي تقرر فيه الآتي:(3)

أ- ما هو محظور خارج الإنترنت هو كذلك عبرها.

ب- إقرار مسؤولية الوسطاء حال الدخول إلى الإنترنت عبر الاتصال بهم لوجودهم في حالة إدراك إيجابي وكذلك حال عدم اتخاذهم موقفاً ايجابياً تجاه العمل غير المشروع مع إمكان قيامهم به، ويمكن القول إن الوسط القانوني الأوروبي برزت به محاولات اعترفت بالبيئة الشاملة للإنترنت ولقد لاقت هذه المحاولات الفقهية نجاحاً وكانت على يد الأستاذ "هيربرت بوركيرت" الذي كانت له رؤية في مسألة المسؤوليات والحقوق الإلكترونية حيث قسم المسؤوليات إلى صغرى ومتوسطة وكبرى. **الأولى** تناول فيها مسؤولية الفرد الاتصالية،

---

1. والجدير بالذكر أن مزود الخدمة أو الخادم عندنا في ليبيا هي شركة ليبيا للاتصالات والتقنية فهي حلقة الوصل بين حواسيبنا وبين الإنترنت مستخدمة كافة أنواع الاتصال مع الانترنت سواء السلكي أو اللاسلكي. وقد بدأت الشركة بالعمل خلال سنة 1995م.
2. د.عمر محمد بن يونس – الجرائم الناشئة عن استخدام الإنترنت – ط 1 – دار النهضة العربية القاهرة – 2004م-ص64.
3. المرجع السابق – ص 132 .

و**الثانية** تناول فيها مسؤولية الخادم أو مزود الخدمة الذي أعتبره أقرب الأشخاص لتحمل المسؤولية عن الجرائم حيث إن الفاعل لا يمكن التعرف عليه وإن تم التعرف عليه فليس من السهل أن يقدم للعدالة، و**الثالثة** الكبرى وهي مسؤولية الدولة وما يحدث من قلق في البيئة الاتصالية الشاملة وتحديها بقيمنا ومعتقداتنا وأصالتنا وشخصيتنا (1) بل من واجبنا العمل على تعزيز التحدي في الاتصالات لحماية التحدي في الشخصية الإنسانية.

أما في القضاء الأمريكي فمع مراعاة أحكام Save Harbor فإن الأصل إن مزود الخدمة لا يسأل ولا يتحمل أدنى مسؤولية مالم ينص على خلاف ذلك ، على أنه فيما يتعلق بالقضاء الأمريكي فإنه ليس هناك صورة أو صور ثابتة في شكل المسؤولية أو قواعد عامة , ففي إطار العدوان على الملكية الفكرية فإنه تدخل فكرة الأرشفة حيث إن النشر أو الأرشفة تسمح لأي شخص بالاطلاع على محتوياتها وفي أي وقت يشاء لأن هذه المحتويات مخزنة في الإنترنت وباعتبارها نوعاً من التخزين .(2) في حين أدان القضاء الأمريكي في ظل حماية الملكية الفكرية توزيع مشروع برمجيات عبر الإنترنت حيث كان Jeoffrey levy قد أدين من محكمة مدينة Eqgene لأنه خلال سنة 1999م. قام بوضع poste وبشكل غير مشروع برمجيات حاسوب وتسجيلات موسيقية وبرمجيات تسلية وأفلام رقمية على موقعه عبر الإنترنت , ممكناً الغير من إمكانية إنزالها ونسخها على الرغم من شمولها بحقوق النسخ ولقد أدين ليفي لارتكابه جريمة انتهاك عمدي لحقوق النسخ بقصد الربح .(3)

1. د.عمر محمد بن يونس – مرجع سبق ذكره – ص 132.
2. المرجع السابق – ص 512.
3. المرجع السابق – ص511.

ويذهب القضاء الفرنسي كذلك إلى عدم مسؤولية مزود الخدمة حيث يرى إلى أن مجرد قيام مستخدم الشبكة يبث رسالة غير مشروعة لا يكفي لقيام مسؤولية لمزود الخدمة، وذلك أخذاً في الاعتبار العدد اللانهائي للمشتركين وحجم الرسائل الرهيب، المتداول وبشكل يومي. (1) أي أن عمل مزود الخدمة فني وليس في مقدوره مراقبة المحتوى المقدم، وهذا ما جاء في احكام القضاء الفرنسي وهي قرينة قضائية لعدم الخطاء وهو لا يمكن تصوره افتراضاً. (2) ونكتفي بهذا القدر للحديث عن مسؤولية الخوادم. والآن ننتقل لطبيعة تفتيش الخادم، ويتم بالطريقة العملية الآتية:

1- يتم استلام البلاغ عن الجريمة من المبلغ ويدون ذلك في محضر رسمي.

2- بعد تثبيت البلاغ يتم التنبيه على المبلغ (المجني عليه) من أنه قد يتم تفتيش حاسوبه في حالة عدم التوصل إلى الفاعل وهو استثناءً وهنا يميز بين الاستعانة بحاسوب المجني عليه وبين تفتيشه وذلك لتمكين جهات الضبط والاستدلال من ضبط اسم الخادم الذي من خلاله تم الدخول، وتعني الاستعانة بحاسوب المجني عليه في هذه الحالة. أنه لا يجوز أن يسأل المجني عليه عما ينجم عن هذا الإجراء من آثار قد تظهر أثناء الاستعانة بحاسوبه.

3- الحصول على إذن تفتيش للخادم لمعرفة الخادم الذي انطلق منه النشاط التقني.

4- يجب أن يتم تفتيش الخادم أولاً للقول بصحة التفتيش وذلك للبحث عن الآثار traces الغريبة لمعرفة دخول حركة الهاكر أو غيره.

5- يتم تتبع حركة دخول الهاكر بالعودة بالسير العكسي trace back لطريقة دخوله مع مراعاة الانتقال المادي بين الخوادم وهو ما يستدعي وجود إذن تفتيش ممتد.

6- ولتقريب المسألة لنفترض كمثال على أن الهاكر قام بخط سير بدءً من منزله ثم إلى مقر عمله ثم مكتبة مركزية ثم شركة صرافة ثم مصرف، فخادم المصرف هنا هو الذي تعرض للانتهاك من خلال الدخول إليه عبر خوادم ومضيفات أخرى.

---

1. الجرائم المعلوماتية – بحث على موقع httb/www.wata.eet– تاريخ الزيارة 22 /2010/7 م.
2. نفس المرجع السابق.

7- يتم الحصول على إذن تفتيش لخادم المصرف أولاً وبتفتيشه يتم العثور على آثار بأن الهاكر استخدم خادماً أخر وهو شركة صرافة وبالانتقال المادي بين الخوادم فيتم الحصول على إذن ثان لتفتيش خادم شركة الصرافة.

8- بتفتيش خادم شركة الصرافة وتتبع الآثار للهاكر تبين أنه استخدم خادماً آخر هو خادم المكتبة المركزية فيتم الحصول على إذن تفتيش ثالث لتفتيش خادم المكتبة المركزية (1).

9- بتفتيش خادم المكتبة المركزية والبحث عن الآثار تبين أنه استخدم خادم مقر عمله فيتم الانتقال إلى القاضي من جديد للحصول على إذن تفتيش رابع لتفتيش خادم مقر عمل الهاكر.

10-بعد الحصول على إذن تفتيش خادم مقر عمل الهاكر والبحث عن الآثار يتبين أن الآثار ممتدة إلى حاسوب الجاني في منزله بالعنوان المدون فيتم الانتقال للقاضي للحصول على إذن تفتيش خامس لتفتيش حاسوب الجاني في منزله.

11- يتم الانتقال ومعرفة عنوان منزل الهاكر فيتم تفتيش حاسوبه وضبطه واتخاذ الإجراءات القانونية ضده.

إن هذا المثال يوضح وجود أكثر من إذن تفتيش ووفقاً لقواعد الإجراءات الجنائية المتعلقة بالتفتيش في الجرائم التقليدية، ونلاحظ أن عامل الوقت في الجرائم الافتراضية من الأمور المهمة جداً والتي يجب مراعاتها من قبل القائم بالتفتيش ورغم أن لكل حالة تفتيش إذن تفتيش خاص يتعلق بها وهو الأصل. ولكي يتم مواجهة حالة الاستعجال والخصائص التي يتميز بها الدليل الرقمي وللسرعة في إجراءات التفتيش والضبط فإنه وبطبيعة الحال أن التفتيش يجرى على خوادم متعددة كما رأينا في المثال ذلك أنه أمر طبيعي في الجرائم الافتراضية. ورأينا مع الاتجاه الراجح المبني على أنه يمكن تطوير الإذن بحيث يشمل أكثر من خادم وذلك باللجوء إلى صيغة إذن امتداد للتفتيش (2) المقررة في المذكرة الإيضاحية لمشروع قانون الجرائم الافتراضية والدليل الرقمي الليبي في الخادم الذي يتـــم

1- مشروع المذكرة الايضاحية لمشروع قانون الجرائم الافتراضية – مرجع سبق ذكره
2- نفس المرجع السابق .

التعرف عليها دون الحاجة لاستصدار إذن جديد (1)، بحيث يمكن الحصول على إذن تفتيش واحد لخادم واحد ويتم تدوين العبارة التالية داخل إذن التفتيش الموجود بمحضر التحقيق وهي ((يتم تفتيش الخادم المعني وكذلك أي خوادم يتبين من السير العكسي أن الانتهاك تم من خلال عبورها(2) حيث إن باقي الخوادم لا يتم التعرف عليها إلا من خلال الخادم الذي تم منه الانتهاك أو الاختراق أو الذي ارتكبت منه الجريمة. (3) على أنه يجب مراعاة الخوادم الموجودة في المساكن الخاصة فيتم الحصول على إذن تفتيش خاص في هذا الشأن. وهو ما يجعل القواعد العامة للتفتيش قائمة باستمرار)).

ولتنفيذ ذلك يجب أن تكون هناك دلائل وقرائن تستدعي تتبع الحركة بين الخوادم أو أي آثار تفيد في كشف الجريمة ويتم توضيح هذه الدلائل والقرائن عند الانتقال لقاضي التحقيق للحصول على إذن تفتيش ممتد. وقد نص على هذا المعنى في مشروع قانون الجرائم الافتراضية والدليل الرقمي في نص المادة (82) حيث نصت على الآتي ((يكتفى بإذن تفتيش واحد إذا كان هناك دلالة تستدعي تتبع مسار الجريمة بالانتقال المادي بين الخوادم في أماكن مختلفة ولا تسري هذه المادة إذا كان بين هذه الأماكن حواسيب أو خوادم في مساكن خاصة، ويراعى مبدأ التعاون الدولي والثنائي والإنابة القضائية في إطار التفتيش خارج الحدود الليبية، إذا كان لذلك حاجة)) (4)

ثانياً / تفتيش مسار الإنترنت وحركة البيانات:

تعد مراقبة مسار الإنترنت وحركة البيانات نوعاً من التفتيش الذي يجرى في العالم الافتراضي وأن المبدأ الذي يحكم المراقبة في هذا الإطار (أن المجرم غالباً ما يعود إلى مكان جريمته) إلا أن هذا المبدأ ليس مطلقاً وتتعدد أسباب ذلك منها إن مكان الجريمة هو هدف سهل للسرقة أو الاختلاس أو لشعور المجرم بعدم وجود رقابة أو برامج تحد من حركته على مسار الإنترنت أو إن هناك أموراً نفسية تتعلق بإبراز جانب البطولة

1- مشروع المذكرة الايضاحية لمشروع قانون الجرائم الافتراضية – مرجع سبق ذكره
2- نفس المرجع السابق .
3- نفس المرجع السابق .
4- مشروع قانون الجرائم الافتراضية والدليل الرقمي – مرجع سبق ذكره .

والتفوق (نظرية البطولة في العالم الافتراضي في دراسات علم الإجرام الافتراضي) على برامج الحماية المعدة للمواقع والأجهزة. والمراقبة كفكرة أساسية مأخوذة من مفاهيم أمن المعلومات، لذلك يفهم أن مدة المراقبة غير محددة فقد تستمر شهوراً قد تطول حتى سنوات يتوقف ذلك على نوع الجريمة وآثارها [1] وأن هناك ما يبرر هذا الإجراء. والجدير بالذكر أن مراقبة مسار الإنترنت وحركة البيانات تؤدي إلى ضبط المجرم وليس الجريمة. ولقد أثارت مراقبة مسار الإنترنت وحركة البيانات العديد من الإشكاليات المتعلقة بحماية الحق في الخصوصية ومنها الاتفاقية الأوروبية للجـريمة الافتراضـية (بودابست – نوفمبر-2001 م) والحقيقة أن مسألة مراقبة مسار الإنترنت لا تعتبر مشكلة في القانون الأمريكي [2] خاصة بعد صدور القانون الوطني الأمريكي في 2001/10/26م. والذي توسع في المراقبة مستنداً إلى تعديل القسم (1030) بالموسوعة الأمريكية. وكذلك توسيع الصلاحيات الممنوحة لمكتب المباحث الفيدرالية الأمريكية FBI بحيث امتدت هذه الصلاحيات إلى خارج الولايات المتحدة الامريكية. ولأهمية الحق في الخصوصية ولأنه حق موضوعي فقد لوحظ أن الضمانات المتوفرة في الإجراءات التقليدية غير كافية فتم اتخاذ مبادرات جديدة لضمان احترام حقوق الإنسان. ومن ذلك مشروع الجرائم الافتراضية والدليل الرقمي في ليبيا والذي نص في المادة (80) منه على أنه " ليس لقاضي التحقيق تفويض الغير في إصدار إذن التفتيش " باعتبار أن المراقبة هي نوع من التفتيش فهي ضمانة إجرائية وفق هذا النص يملكها قاضي التحقيق وحده دون غيره وهي من الضمانات الرئيسية التي تحافظ على حقوق الإنسان كما تمنح الثقة لرجال القضاء والدفاع عن حقوق الفرد.

1- مرجع سبق ذكره .
2- مرجع سبق ذكره .

ولكن كيف يتم مراقبة مسار الإنترنت لضبط المجرم؟ سواء ارتكبت واقعة معينة أو إذا عاد المجرم إلى مكان جريمته السابق؟

وللإجابة عن ذلك نقول إن الواقعة التي يكون فيها الجاني يرتكب الجريمة وهو مراقب فهي حالة تلبس حسب القواعد العامة، أما إذا عاد الجاني إلى مكان جريمته لأنه ارتكب جريمة قبل ذلك ويكون مسار الإنترنت مراقباً من قبل السلطات فهي تعتبر حالة تلبس أيضاً، والغرض هنا تداخل إجراء التحقيق في إجراء الاستدلال، فمراقبة حركة مسار الإنترنت هو إجراء من إجراءات التحقيق وليس استدلالاً والغرض منه التعرف على مرتكب الجريمة.

وقد تناول مشروع الجرائم الافتراضية والدليل الرقمي في نص المادة (81) الحالتين حيث نصت المادة على الآتي " يجوز تحت إشراف قاضي التحقيق مراقبة النظام التراسلي والشبكات والحواسيب المشتركة ومزودي الخدمات بقصد التوصل إلى الجريمة ومرتكبها ويصدر قاضي التحقيق إذناً بالمراقبة بعد سماع أقوال ممثل الجهة القائمة بالمراقبة، ويجوز الاستعانة بخبير استشاري لأداء مهمة المراقبة، وفي هذه الحالة يتولى الخبير أو الاستشاري القيام بالمراقبة تحت إشراف قاضي التحقيق مباشرة "(1)

ويفهم من الفقرة الأولى من المادة (81) أن مراقبة الإنترنت والشبكات والحواسيب ومزودي الخدمة بقصد التوصل إلى الجريمة وفاعلها يتم تحت إشراف قاضي التحقيق وهو الذي يصدر الإذن بالمراقبة بعد أن يسمع أقوال الجهة المعنية القائمة بالمراقبة، وإذا لم تتوفر الخبرة الفنية فيجوز الاستعانة بخبير أو استشاري يندب لهذا الغرض ويقوم بمهامه تحت إشراف مباشر من قاضي التحقيق، وإذا تم ضبط الجريمة ومكان الجاني تتخذ ضده الإجراءات القانونية. (2)

أما إذا كانت هناك حالة استعجال فيجوز الاعتداد بمحضر ضبط حركة ومسار الإنترنت وهي تماثل حالة التلبس ويجب أن يعرض محضر الضبط بشكل فوري

1- مرجع سبق ذكره .
2- مرجع سبق ذكره .

على قاضي التحقيق لاستصدار أمر باستمرار السير في الإجراءات ومتابعتها أو استصدار أمر بالأوجه لإقامة الدعوى وليس لقاضي التحقيق تفويض غيره في هذه الإجراءات. ([1])

وقد نصت المادة (81) من مشروع القانون في الفقرة الثانية على هذا المعنى " يجوز في حالة الاستعجال الاعتداد بمحضر ضبط حركة ومسار البيانات وتعد حالة الاستعجال هنا في مرتبة التلبس ويلزم في هذه الحالة عرض محضر الضبط فوراً على قاضي التحقيق لاستصدار أمر باستمرار السير في الإجراءات أو استصدار أمر بالأوجه لإقامة الدعوى ("[2])

إلا أنه يجب أن يشمل ملف الدعوى ملفاً فنياً تقنياً يتضمن كيفية إجراء المراقبة وإجراءاتها والقائم بها وزمنها ومن كان حاضراً وكيف تم الدخول ويجوز للسلطات القائمة بالمراقبة لمسار الإنترنت عدم الكشف عن البرامج المستخدمة في الكشف عن الجريمة والجاني إذا كانت هذه البرامج ذات حصانة أمنية في المحكمة وبصورة علنية ويجوز أن يتم إبلاغ قاضي التحقيق أو قاضي الموضوع اذا كانت الجلسة سرية , فإذا تم هذا الاجراء فإن التبرير ملزم في الحكم وعلى السلطات تقديم المبررات لهذا الطلب ,وليس لقاضي الموضوع رفض طلب السلطات ولكن له أن يعقد جلسة سرية أو أكثر للاستماع إلى طلبات السلطات ومعرفة سبب عدم كشفها عن البرامج المستخدمة(3) ولقد جاء هذا المعنى في الفقرة الثالثة من نص المـــادة (81) من مشروع قانون الجرائم الافتراضية حيث نصت أنه " ولا يجوز مباشرة الدعوى أو الاستمرار فيها مالم يتضمن ملف الدعوى تقريراً تقنياً مفصلاً لهذه المراقبة المسبقة التي أسفرت عن الكشف عن الجريمة ومرتكبها , ويجوز للسلطات التقرير بسرية تقنية أو غيرها تم استخدامها في المراقبة وعدم الكشف عنها في المحكمة (4). اما طبقاً للقواعد العامة فان قانون الاجراءات الليبي لم يشترط في مباشرة الدعوى تقرير مفصل عن الواقعة حسب نص المادة (51) وكذلك في الاحالة في الجنايات والجنح والمخالفات واجاز القانون اجراء تحقيقات تكميلية بعد الاحالة نص المادة (166) للنيابة العامة تقديم المحضر الى المحكمة المختصة.

1- مشروع المذكرة الايضاحية لمشروع قانون الجرائم الافتراضية – مرجع سبق ذكره .
2- المرجع السابق .
3- نفس المرجع السابق .
4- المرجع السابق

ومن خلال ما تقدم نلاحظ أن هناك ضمانات إجرائية لحق موضوعي وهو حق الخصوصية وأعطى السلطة القانونية لقاضي التحقيق وليس لأحد غيره. وكمثال على تفتيش مسار الإنترنت وحركة البيانات نذكر قضية أشهر الهكرة وهو Kevin Mitnick وعلى الرغم من التقنية العالية التي تملكها أجهزة الضبط الأمريكية فلم يكن من السهل الوصول إلى تحديد شخصيته ومعرفة تحركاته عندما تدخل هاكر آخر يعمل معيداً في جامعة كاليفورنيا يدعى Tsutomu Shimomura وهو أستاذ حاسوب ويعمل خبير أمن. والذي أخذ على عاتقه تتبع آثاره وضبطه بعدما وجه إليه سب عبر البريد الصوتي voicemail(1) وبالفعل تمكن من خلال برمجيات خاصة لتتبع المصدر من حواسيبه العاملة ومعرفة تحركات Mitnick وأبلغ المباحث الفيدرالية في ديسمبر 1994م. حيث بدأت آثاره واضحة من خلال قيام Mitnick بانتحال الشخصية عبر الإنترنت ونسخ الملفات الأمنية من حواسيب Shimomura, وبالطبع لاحظ Mitnick برمجيات تقصي وتتبع المصدر فترك رسالة سب وقذف ل Shimomura مما جعل الأخير يتخذ منه موقفا شخصيا مضاداً وبالفعل توصل إلى تقصي ومعرفة من اخترق حاسوبه وفي 1997م. أدلى Shimomura بشهادته أمام اللجنة العلمية في الكونجرس الأمريكي (2) وفرض القضاء الأمريكي عقوبة منع التعامل بالتقنية الحديثة على Kevin Mitnick وذلك لارتكابه جرائم خطيرة للغاية منها اختراق شبكات عالمية واستخدام برمجيات تقصي وكشف كلمات العبور وانتحال الشخصية وحكم عليه بالسجن لمدة خمس سنوات وأطلق سراحه سنة 2000م.(افراج شرطي). وانتهت علاقته بالنظام القضائي ويعمل حالياً مستشاراً في كبرى المؤسسات المتخصصة في صناعة تكنولوجيا المعلومات (3) وقد تناول المشرع الليبي مراقبة مسار الإنترنت ومزودي الخدمة في قانون الاتصالات الحديث رقم 22 لسنة 2010م. بشـــأن الاتصالات في نص المادة (14) على أنه " تقوم الجهة المختصة بالتحقق من التزام

1- د. عمر محمد بن يونس – المجتمع المعلوماتي – مرجع سبق ذكره – ص 46
2- المرجع السابق –ص47
3- المرجع السابق –ص 48

المشغلين ومزودي الخدمة بشروط التراخيص وأحكام التشريعات ذات العلاقة، وعلى الأخص ما يلي:

1-الكشف على مواقع الشبكات وأجهزة الاتصالات المستعملة.

2-التأكد من سلامة الأنظمة المتبعة لإصدار قوائم الحساب ودقتها.

3-التأكد من مستوى الخدمات المقدمة لطالبيها وبحث ما يقدم من شكاوى في شأنها

4-التأكد من حسن إدارة المشغل أو المزود للخدمة المرخص بها. (1) ويلاحظ ان المشرع هنا استخدم مصطلحات غير مفهومة بالتحديد الذي يؤدي الى قاعدة التفسير والبحث.

وكذلك تناول سرية الاتصالات والحق في الخصوصية في نص المادة (15) حيث نصت على أنه " على الجهات التي تقدم الخدمات اتخاذ كافة الخطوات لضمان سرية اتصالات المستفيدين ولا يجوز للجهات التي تقدم الخدمات اعتراض أو مراقبة أو تغيير أو تعديل اتصالات المستفيدين من الخدمة " وفي إطار مبدأ حماية المعلومات الشخصية تنص المادة من نفس القانون على أنه " تكون الجهة التي تقدم الخدمات مسؤولة عن المعلومات المتعلقة بالمستفيد التي تكون بحوزتها أو بحوزة وكلائها ويجب عليها حماية معلومات اتصالات المستفيدين بوسائل الحماية الأمنية ومراعاة الخصوصية , ولا يجوز لها جمع أو استعمال أو حفظ أو إفشاء معلومات أو اتصالات المستفيد لأي غرض إلا في حدود المسموح بها قانوناً أو بموافقته الشخصية وفي الأغراض التي تمت من أجلها " [2] ونلاحظ أن القانون رقم 22 لسنة 2010م بشأن الاتصالات الليبي . قد أرسى مبدأ مراقبة مسار الإنترنت والحق في الخصوصية وسرية الاتصالات بكافة أنواعها.

ثالثاً / تفتيش حاسوب المتهم:

تختلف الجرائم الافتراضية عن الجرائم التقليدية في شخصية المجرم واساليب تنفيذ الجريمة، لان المجرم لديه دراية تقنية ولذلك يجب التمييز بين مجرم الإنترنت ومجرم الحاسوب، فمجرم الإنترنت المتميز هو الهاكر HACKER أما مجرم الحاسوب فهو القرصان PIRATE وأغلب الجرائم التي يرتكبها هي تتعلق بالعدوان على حقوق الملكية

1. القانون رقم 22 لسنة 2010م بشأن الاتصالات – مدونة التشريعات – السنة 10 – العدد 10- منشورات مؤتمر الشعب العام
2. نفس المرجع السابق

الفكرية بالإضافة إلى إساءة استخدام الحاسوب مثل اختراق كلمات العبور الملفات مشفرة مخزنة في الحاسوب STAND ALONE COMPITER أي ان يكون الحاسوب غير مرتبط بالإنترنت (1).

ولقد اعتمد القضاء الأمريكي معيار الهكترة بكونه يعتبر من المهارة الخاصة SPECIAL SKILLS فالهكترة إذن هي مستوى من المهارات الخاصة يتمتع بها الهاكر ويدل على الكفاءة والدراية التقنية ويملك قدرات خاصة في ارتكاب أفعال في العالم الافتراضي لا يستطيع القيام بها عامة الناس. وقد ميز القضاء الأمريكي نوعين من الهاكر الأول هو الهاكر الأمن HACKER وهو الذي يتمتع بقدرات تقنية في الاختراق ويسبح في عالم البيانات وهو غير مؤذي وهدفه الحرية المطلقة في العالم الافتراضي. والنوع الثاني وهو الأخطر ويسمي الكراكر CRACKER وهو المخترق من ذوي النوايا الإجرامية وبرز هذا المصطلح خلال سنة 1985م. وهو يمثل التهديد المباشر للإنترنت (2) تفتيش حاسوب الجاني تعتبر الخطوة الثالثة ضمن الخطوات التي يجب اتباعها طبقاً لنظرية التفتيش في الجرائم الافتراضية، ومعلوم أن المقصود بحاسوب المتهم أي الذي

يكون تحت حيازته سواء أكان هذا الحاسوب ضمن محتويات مكتبه أو منزله أو داخل المؤسسة التي يعمل بها أو كان الحاسوب ضمن أمتعته أو حقيبته (حاسوب محمول)، يمكن لرجال سلطة التحقيق اتخاذ إجراءات لضبط حاسوب المتهم وهي إجراءات مادية تفرضها بعض الوقائع والتي منها على سبيل المثال أن تطلب سلطات التحقيق غلق التيار الكهربائي على المكان الذي يوجد به حاسوب الجاني ولو كان موجوداً في مؤسسة عامة (3)، لأن هذا الإجراء المادي له دور هام في حماية الدليل الرقمي من التلف الذي يمكن أن يتسبب به الجاني , لأن المجرم في الجرائم الافتراضية في أغلب الأحوال يكون محترفاً وعلى دراية تقنية تامة وقد يضع برامج وأدوات رقمية تهدف إلى إتلاف الأدلة في نظام الحاسوب الخاص به والإجراءات المادية التي تتخذها السلطات بإغلاق التيار

---

1. دعمر محمد بن يونس – السلوك الإنساني المخاطب بالقاعدة الموضوعية في القانون الجنائي – بحث مقدم إلى ندوة الجريمة الافتراضية في التشريعات العربية – شرم الشيخ مصر –خلال الفترة من 24-2007/4/26م
2. د.عمر محمد بن يونس – بحث بعنوان مجرم الانترنت – الجمعية العربية لقانون الانترنت – غير منشور.
3. مشروع المذكرة الإيضاحية – مرجع سبق ذكره.

الكهربائي تجعل الحاسوب يتوقف عن العمل ولتستطيع السلطات المختصة تنفيذ إذن التفتيش وضبط الحاسوب وتفتيشه أثناء فترة إغلاق التيار الكهربائي، وبالتالي ضبط الجاني إذا أمكن ذلك (1). وعند اتخاذ هذه الإجراءات يجب أن نميز بين الحاسوب المنفرد STANDALANE COMPITAR والحاسوب المشمول بالحماية PROTCTED COMPITER من حيث الخطوات التي يجب أن يتخذها الخبير التقني عند إجراء التفتيش، كذلك هل الحاسوب في ملكية أو حيازة الجاني؟

- التمييز بين الملكية والحيازة:

يلزم التمييز قانونا بين ملكية الحاسوب ومثالها الحاسوب الشخصي للجاني في مكتبه الخاص أو منزله أو كان يحمله وهو ملك له , وارتكب به جريمة سواء أكان منفرداً أو مشمولاً بالحماية , وبين الحيازة ومثالها الحاسوب الموجود في المؤسسة العامة أو الشركة الخاصة أو مقهى الإنترنت فهو حين يرتكب به الجاني جريمة تحت حيازته ولكنه ليس ملكاً له أي أنه مستخدم للجهاز فقط ومثالـــها موظف يعمل في مصرف قام باستخدام الحاسوب لسرقة أو اختلاس مبالغ مالية من مجموعة حسابات للزبائن فهذه الجريمة وقعت بحاسوب جهة العمل ولكن الحاسوب تحت حيازة الموظف وبرقم دخوله إلى المنظومة (2) وهناك نوع آخر من الملكية وهو الملكية المشتركة ونعني به امتلاك العديد من الأشخاص لذات الجهاز ، فماهي النتائج المترتبة على هذا التمييز بين أنواع الملكية والحيازة وللإجابة نقول إن مالك الحاسوب يمكنه أن يأذن بتفتيشه للسلطات (الرضاء بالتفتيش) طالما لديه السيطرة التامة على الحاسوب (3) وقد يتم إجراء التفتيش بناء على إذن تفتيش من القاضي SEARCH WARRANT أما الحيازة للحاسوب فيجوز لحائز الجهاز منح الإذن بتفتيشه أو بناء على موافقة صاحب العمل EMPLOYER أو أي موظف له سلطة إدارية قانونية أو ظاهرية ، ويمكن إجراؤه بغير إذن ويتوقف ذلك على التمييز بين الوقائع وقد قررت المحكمة العليا الأمريكية في قضية OCONNOR.VORTEGE سنة 1987 م الشهيرة بقضيةOCONNOR حيث قضت (إن شرعية تفتيش مقر العمل

1- مشروع المذكرة الإيضاحية – مرجع سبق ذكره.

2- ومن الأخطاء الشائعة في تفتيش الحاسوب الذي في حيازة موظف هي الاعتماد على نظام التشغيل في إبراز أو كشف الجرائم ولذلك لا يجوز استخدام نظام التشغيل في أجهزة الحاسوب مثل HASTER لكشف الدليل حيث إنه إجراء يشوبه البطلان.

3- د.عمر بن يونس – الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي – مرجع سبق ذكره-ص 89

بغير إذن تعتمد في الغالب على التمييز بين التدقيق للوقائع ، كما لو كان مقر العمل قطاعاً عاماً أو خاصاً وما إذا كانت سياسات التوظيف يتوافر فيها ما يسمح بالتفتيش وما إذا كان التفتيش مرتبطاً بالعمل)(1) أما الملكية المشتركة فقد تعرض لها القانون الأمريكي وأجاز تفتيش الحاسوب الذي يملكه مجموعة أشخاص لأن جميعهم يفترضون خطورة قيام المستخدم المشترك CO-USER باكتشاف كل شيء والاطلاع عليه داخل الحاسوب وبما يسمح بتفتيش هذه الأجهزة (2) وفي أحكام المحكمة العليا الأمريكية التي صدرت في قضية MATLOCKوالتي قضت فيها (إن الفرد لديه سلطات مشتركة على عقارات أو ممتلكات يمكنه إبداء الموافقة على إجراء التفتيش ولو كان المستخدم رافضا لذلك (3) ولهذا فطبقا لرأي المحكمة العليا فإن السلطة المشتركة هي التي تؤسس حق الطرف الثالث في الموافقة تتطلب في الواقع الاستخدام المشترك للحاسوب المملوك بواسطة الأشخاص الذين يقومون بالسيطرة المشتركة عليه، إن للمشتركين في استخدام الحاسوب بصفة عامة الحق في إصدار الموافقة على تفتيش الملفات المخزنة في الحاسوب المشترك وفقا لقرار المحكمة العليا في قضية MATLOCK وتوصل القضاء أيضا إلى أن المرأة يمكنها الموافقة على تفتيش حاسوب زوجها الموجود داخل منزلهما ، ويجب ملاحظة أنه إذا استخدم أحد المشتركين في ملكية الحاسوب كلمات سر تحمي بعض الملفات الخاصة به فلا يجوز للمشتركين معه الإذن بتفتيش هذه الملفات ، وقد قررت الدائرة الرابعة للمحكمة الأمريكية أن سلطة هؤلاء المستخدمين الآخرين للموافقة على تفتيش الحاسوب لا تمتد إلى الملفات التي تحميها كلمة السر ، وفي حكم للقضاء الأمريكي (**قرر تشبيه الملفات التي تحميها كلمة السر بالأدراج المغلقة داخل حجرة النوم**)(4) أما إذا حصلت المرأة المشتركة في الاستخدام على كلمة السر من زوجها فيجوز لها الموافقة على تفتيش الملفات وفقا لمنطق قضية MATLOCK .

1- المرجع السابق – ص 127.
2- نفس المرجع السابق – ص 87
3- د. عمر محمد بن يونس – الإجراءات الجنائية - مرجع سبق ذكره – ص 98
4- المرجع السابق – ص90

ولذلك يجب أن يلاحظ القائم بالتفتيش هذه الأمور ويوثقها في محضر التفتيش لما لها من آثار في الدفع بالبطلان(1), ويجب أن يدرك الشخص القائم بالتفتيش الغاية والهدف الذي يسعى إليه , من اتخاذ إجراءات ضبط وتفتيش حاسوب الجاني وبالتالي مرتكب الجريمة وهذا الأمر يحتاج من القائم بالتفتيش إلى توثيق المعادلة ما بين التفتيش بقصد الوصول إلى مرتكب الجريمة الافتراضية , وبين استخلاص الدليل , وهذا الأمر يعتبر على درجة كبيرة من الأهمية ويرتب الكثير من الآثار القانونية بما في ذلك الجرائم العرضية التي قد تظهر أثناء تفتيش الخوادم بقصد الوصول إلى حاسوب الجاني , وقد ورد هذا المعنى في نص المادة (39) إجراءات جنائية ليبي حيث نصت على أنه " لا يجوز التفتيش إلا للبحث بين الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها ، ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشياء تعد حيازتها جريمة أو تفيد في كشف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائي أن يضبطها "(2)

ومن ضمن الإجراءات التي تتخذها سلطة التحقيق عند تفتيش حاسوب الجاني أنه يتم التحفظ على الحاسوب بطريقة تسمح باستخدام النظم المتطورة في إجراءات التفتيش التقني، ويجب أن يتم مباشرة إجراءات التفتيش لحاسوب الجاني من قبل خبرة متخصصة ومحلفة ولا يتم التفتيش من سلطة التحقيق أو من مأمور الضبط القضائي (3) على أنه يجب مراعاة أن التحفظ على حاسوب الجاني لا تزيد مدته على ثلاثة أشهر في أفضل الظروف مما عدا الجرائم المرتكبة ضد أمن الدولة وشخصيتها وقد نص على ذلك في مشروع قانون الجرائم الافتراضية الليبي.

وإذا تأملنا منطق التفتيش التقني المتطور والذي يجريه المختصون على حاسوب الجاني بهدف استخلاص الدليل فإنه يجب اتباع التقنيات الحديثة في هذا الإطار مثل نظم BITSTREAM (4) وغيرها من النظم المتطورة. لذلك يجب أن تتعامل سلطات التحقيق مع حاسوب المتهم على أنه

1- د. عمر محمد بن يونس – الإجراءات الجنائية - مرجع سبق ذكره – ص 91
2- مجموعة التشريعات الجنائية -الجزء الثاني – الإجراءات الجنائية-منشورات الإدارة العامة للقانون – ليبيا 1987 م- ص13.
3- مشروع المذكرة الإيضاحية – مرجع سبق ذكره.
4- وهو جهاز حاسوب ذو امكانيات تقنية عالية يستخدم في المعامل الرقمية عند الكشف عن الحواسيب وانظمتها وما تحويه من ملفات وبيانات ووظيفته انشاء نسخة تحاكي النسخة الاصلية للجهاز المضبوط لمحتويات أي حاسوب وكأنها مرآة بحيث يتم الكشف عن النسخة الثانية دون المساس بالأصل خوفاً من اتلافها اثناء العمل عليها.

الحاسوب الذي سوف يتم استخلاص الدليل منه وتراعي عند ضبطه وتحريزه الإجراءات التقنية والفنية عند الضبط والتحريز والنقل للمعامل الشرعية لاتخاذ إجراءات التفتيش (1). وقد وردت هذه الإجراءات التي يجب أن تتخذها سلطات التحقيق في نص المادة (81) من مشروع قانون الجرائم الافتراضية حيث نصت على أنه " يجوز اتخاذ إجراءات مادية لضبط حاسوب المتهم دون المساس بحقوقه التي يقرها القانون , ويلـزم التحفظ على حاسوب المتهم بطريقة تسمح باستخدام النظم المتطورة في التفتيش التقني , وتتم مباشرة إجراءات تفتيش حاسوب المتهم من قبل خبرة متخصصة محلفة , وفيما عدا الجرائم المرتكبة ضد أمن الدولة وشخصيتها فإنه ليس في هذا القانون ما يبرر التحفظ على القطع الصلبة لحاسوب المتهم لأكثر من ثلاثة شهور"(2).

إن تفتيش وضبط حاسوب المتهم من الخطوات المهمة التي يجب أن تنفذها سلطات التحقيق وفقاً لطبيعة التفتيش مع مراعاة أن المتهم قد يضع برامج حماية أو شفرات خاصة بأنظمة التشغيل أو برامج تدمير ذاتي للبيانات والمعلومات المطلوب تفتيشها والتأكد منها وهذه المعلومات يجب أن تتأكد منها سلطة التحقيق عند جمع المعلومات والتحريات وفتح محاضر التحقيق بحيث تتفادى حدوث هذه الوقائع عند ضبط حاسوب الجاني وتفتيشه وخاصة عند اتخاذها لإجراءات التفتيش في الجرائم المرتكبة ضد شخصية الدولة أو جرائم الإرهاب ... إلخ.

رابعاً / تفتيش حاسوب المجني عليه:

إن تفتيش حاسوب المجني عليه أو المدعي بالحق المدني واستخلاص الدليل منه هي الخطوة الرابعة في سلسلة الإجراءات للحصول على الدليل وأسلفنا عند بحثنا في الخطوة الأولى وهي تفتيش الخوادم والمضيفات أنه يتم التنبيه على المجني عليه أثناء إعداد محضر التفتيش أنه قد يتم الاستعانة بحاسوبه في حالة جدوى الخطوات السابقة وهي استثناء عن الأصل من أجل استخلاص الدليل وللقيام بهذا الإجراء لابد من توافر شرطين (3) **الأول** موافقة المجني عليه موافقة صريحة ويعتبر البلاغ أو الشكوى التي تقدم

1. مشروع المذكرة الايضاحية.
2. المرجع السابق.
3. نفس المرجع السابق.

بها المجني عليه موافقة على ذلك أو اتخاذ سلطات التحقيق للإجراء دون إبداء الاعتراض منه أو قبول الادعاء بالحق المدني، و**الثاني** أن يكون حاسوب المجني عليه هو المصدر الوحيد للدليل الرقمي إزاء وجود قاعدة عدم تجريم النفس التي يحتمي بها الجاني أي عدم تقديم الدليل ضد نفسه ومثالها عدم تقديم الجاني للرقم السري أو الشفرة الخاصة ببرامج الجهاز وطريقة فتحها وتشغيلها(1)، وإذا توافر الشرطان يخضع الإجراء لقناعة التحقيق وعقيدة قاضي الموضوع , وإذا رفض القاضي الدليل المستمد منه وجب تسبيب الحكم وإلا فقد حكمه المنطق وترتب عليه البطلان بالضرورة .

إن هذا الاستثناء الوارد على القواعد العامة للتفتيش تقرر **ولأول مرة في القضاء العربي المقارن من خلال حكم محكمة جنح العطارين** (2) (الإسكندرية بجلستها العلنية يوم 2003/9/22م. في قضية النيابة العمومية رقم 2001/6319 جنح العطارين). حيث لم يرد هذا المبدأ في أي قضاء مقارن. حيث إن النيابة العامة أسندت إلى المتهم أنه بتاريخ 2000/12/21م. بدائرة قسم العطارين اعتدى على حق من حقوق المؤلف المجني عليه محمد ابوبكر بن يونس بأن نسخ مصنفات عنه بدون إذن كتابي سابق منه.

وقد جاء في حيثيات حكم المحكمة الآتي (وإذ تطمئن المحكمة بثبوت هذا الفعل قبل المتهم وذلك مما انتهت إليه في تقرير اللجنة الثلاثية التي قامت بمراجعة ما ورد بالمصنف الخاص بالمدعي بالحق المدني على الديسكات محل الفحص على الحاسب الآلي الخاص بالمدعي بالحق المدني **والذي تشير المحكمة إلى صحة هذا الإجراء** نظراً لرفض المتهم تقديم الرقم الكودي لفك شفرة الديسكات سالفة الذكر) (3). من خلال هذا الحكم وهو يعتبر سابقة في القضاء المقارن أن المحكمة أقرت بصحة الإجراء التي اتخذته سلطات التحقيق فيما يتعلق باستخلاص الدليل من حاسوب المجني عليه (المدعي بالحق المدني هنا) وعللت ذلك بأن الجاني رفض تقديم الأرقام السرية لفك شفرة الديسكات موضوع القضية، أي أنه المصدر الوحيد للدليل الرقمي في الواقعة هو حاسوب المجني عليه بالإضافة إلى موافقة المجني عليه على استخلاص الدليل من حاسـوبه وهما

1- مشروع المذكرة الإيضاحية – مرجع سبق ذكره .
2- المرجع السابق .
3- المرجع السابق .

الشرطان الأساسيان لاستخلاص الدليل من حاسوب المجني عليه وقد ورد ذلك بالنص الصريح في مشروع قانون الجرائم الافتراضية والدليل الرقمي في نص المادة (83) على أنه " ليس في هذا القانون ما يبرر تفتيش حاسوب المجني عليه. وعلى استثناء يجوز تفتيش حاسوب المجني عليه إذا كان هو السبيل الوحيد لاستخلاص الدليل وقبل هو ذلك كتابة في محضر رسمي.

ويلاحظ على النص السابق أنه أقر بعدم وجود مبرر لتفتيش حاسوب المجني عليه إلا في حالات استثنائية وإذا كان هو السبيل الوحيد لاستخلاص الدليل واشترط أن يتم ذلك كتابة في محضر رسمي يبدي فيه المجني عليه الموافقة واضحة وصريحة (1) لذلك يتضح أن استخلاص الدليل من حاسوب المجني عليه هو استثناء تفرضه بعض الوقائع وهي محددة بعينها ويجب التقيد من قبل المحكمة بالشروط التي ذكرناها وهي موافقة المجني عليه وكون حاسوب المجني عليه هو المصدر الوحيد للدليل الرقمي أي إن كافة الخطوات السابقة تم اتخاذها ولم تحقق نتيجة , ولم يتم الحصول على الدليل الرقمي.

---

1. مشروع المذكرة الإيضاحية لقانون الجرائم الافتراضية الليبي – مرجع سبق ذكره.

الفرع الثاني

التفتيش الرقمي

يلزم وعند إجراء تفتيش الحواسيب أن نفرق بين حالتين في وضعية عمل الحاسوب وهما:

1- **الحالة الأولى:**

حالة الحاسوب المنفرد STAND ALONE COMPUTER وهو الحاسوب غير المرتبط بشبكة الإنترنت .ويكون أداة لتخزين البيانات والمعلومات فقط ، وقد وفرت له أغلب القوانين في العالم الحماية الجنائية اللازمة استنادا إلى مبدأ الحق في الخصوصية مما يستدعي معه الحصول على إذن تفتيش (1) SEARCH WARRNT من سلطة التحقيق للقيام بضبط الأدلة والمحافظة عليها وهو إجراء مختلف عن الإجراءات التي تتخذ في حالة الحاسوب المرتبط بالشبكة ، لذلك يجب مراعاة التخصيص في إذن التفتيش واعتبار الحاسوب المنفرد ضمن متعلقات المكان الذي صدر الأمر بتفتيشه (نص المادة 39 من قانون الإجراءات الجنائية الليبي – لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها) سواء كانت حالة تلبس أو في حالة الحصول على إذن تفتيش (2) او عند تفتيش منازل الاشخاص الموضوعين تحت مراقبة الشرطة والمشتبه في امرهم او المشردين الذين ليس لهم محل اقامة ثابت في ليبيا وهو ما يقودنا إلى إمكانية تطبيق نص المادة (36) إجراءات ليبي التي تنص على تفتيش منزل المتلبس بالجريمة وكذلك نص المادة(35) إجراءات جنائية ليبي التي تنص على تفتيش المقبوض عليهم ، وتطبيق قاعدة أنه كلما أجاز القانون القبض على شخص أمكن تفتيشه وما بحوزته (3) من أشياء أو أمتعة وقد يكون الحاسوب المحمول إحداها أو موجوداً داخل سيارته الخاصة والتي يقودها أثناء ضبطه من قبل مأموري الضبط القضائي ،

1- د.عمر محمد بن يونس – الجرائم الناشئة – مرجع سابق ذكره – ص 858.
2- المرجع السابق – ص 859.
3- انظر البند المتعلق بالتمييز بين الحيازة والملكية في الفرع الاول السالف.

ولهذا يمكن لسلطات التحقيق إجراء التفتيش المادي على القطع الصلبة أو ملحقات الجهاز (الحاسوب المنفرد) أو الوسائط التقنية الأخرى المستخدمة في أداء وظيفته، وهو يختلف عن التفتيش الرقمي الذي يتم بواسطة النظام التراسلي TCP/IP .

والتفتيش المادي على الحاسوب المنفرد نصت عليه المادة (84) من مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا حيث جاء فيها (يجوز اتخاذ إجراءات مادية لضبط حاسوب الجاني دون المساس بحقوقه التي يقررها القانون ويلزم التحفظ على حاسوب الجاني بطريقة تسمح باستخدام النظم المتطورة في التفتيش التقني) (1).

2- **الحالة الثانية:**

الحاسوب المشمول بالحماية PROTECTED COMPUTER ويقصد به كل حاسوب مرتبط بالإنترنت وبأي طريقة والتفتيش الذي يجرى في هذه الحالة هو التفتيش الرقمي ويقصد به تتبع حركة مرتكب الفعل الإجرامي عبر الخوادم والمضيفات لغرض الوصول تقنياً للحاسوب الذي استخدم في ارتكاب الجريمة أو الجرائم عبر العالم الافتراضي (2) وقد يكون الحاسوب في مكان وتتحقق نتيجة الجريمة في مكان آخر يبعد ألاف الأميال ، ويعد التفتيش الرقمي بالتحديد إذا تم باستخدام النظام التراسلي أو الحزمي TCP/IP وقد وضعت المادة 80 من مشروع قانون الجرائم الافتراضية والدليل الرقمي في ليبيا حظراً على عدم التفويض في إصدار إذن التفتيش ولا إجرائه بشكل عام ما لم يكن مقرراً بشكل رقمي ويجب تحديد المسار الذي تم من خلاله التفتيش الرقمي حيث تنص المادة المذكورة على الآتي (لا يجوز التفويض في إصدار إذن التفتيش تنفيذا لهذا القانون ، ولا يجوز إصدار إذن تفتيش عام ما لم يكن التفتيش مقررا بشكل رقمي ، وفي هذه الحالة يجب النص في إذن التفتيش على الغاية منه بشكل واضح وصريح ومباشر وبحيث يشتمل أيضا على تحديد المسار الذي يتم من خلاله التفتيش الرقمي،

---

1. د.عمر محمد بن يونس – مرجع سبق ذكره – ص 859
2. مشروع قانون الجرائم الافتراضية – مرجع سبق ذكره

ويعد التفتيش رقميا إذا تم باستخدام النظام التراسلي فقط وبما يستدعي ذلك تتبع حركة مرتكب الجريمة عبر الخوادم والمضيفات بقصد الوصول إلى الحاسوب الذي انطلق منه النشاط التقني في الجريمة) (1). ويلاحظ على نص المادة السابقة انها بالغت في الالفاظ التي تدل على الغاية من اذن التفتيش وضرورة بيانه بشكل دقيق ، ومن الناحية العملية وعند إجراء التفتيش في **الحالة الأولى** وهو الحاسوب المنفرد يمكن أن تكون الحواسيب في مكان واحد أو في عدة أماكن داخل المؤسسة العامة أو الشركة او غيرها ... الخ ، أما **الحالة الثانية** فإن إجراء التفتيش فيها وهو التفتيش الرقمي يستدعي تتبع حركة البيانات عبر الخوادم والمضيفات مما يتطلب معه الانتقال المادي إلى عدة أماكن مختلفة لغرض معرفة الحاسوب الذي انطلق منه النشاط التقني (2) وبالتالي فإن إذن التفتيش SEARCH WARRANT لمكان واحد قد لا يجدي نفعا في الحصول على الدليل الرقمي ويتطلب أن يكون التفتيش الرقمي ممتداً إلى كل الأماكن التي وجدت بها آثار TREES وهو ما سنبحثه لاحقا وقد يصعب على السلطات التتبع المادي لآثار الجريمة الافتراضية خاصة إذا كانت الخوادم خارجة حدود الدولة ، لذلك يذهب رأي إلى تطبيق تشريعات الطوارئ والتي من خلالها يمكن تتبع مسار الإنترنت عن بعد ومنها القانون الوطني الأمريكي الذي أجاز إجراء التفتيش عن بعد واستخدام الإنترنت في تتبع الدليل الرقمي (3).وقد حدث هذا فعلا في الولايات المتحدة الأمريكية عندما أعدت برنامجاً يدعى (كارنيفور) أو دعته في الخوادم والمضيفات حول العالم .

1- مشروع الجرائم الافتراضية – مرجع سبق ذكره .

2- مشروع الجرائم الافتراضية – مرجع سبق ذكره .

3- د. عمر محمد بن يونس – الدليل الرقمي – ط 1 – منشورات الجمعية العربية لقانون الانترنت – القاهرة – 2008م – ص 70.

المطلب الثالث

قابلية مكونات الحاسوب المنطقية

تمهيد وتقسيم /

إن التطور العلمي هو إنجاز للإنسانية بكل المقاييس وهذا التطور قد أثر وبشكل مباشر في أهمية المعلومات وخصوصا في المجال الاقتصادي والمالي ، بعدما أصبحت المعلومة يمكن إرسالها واستقبالها في ثوان معدودة في أنحاء العالم وعلى مختلف الأشكال والأحجام ، وقد تناول فقهاء القانون الجنائي قابلية مكونات الحاسوب للتفتيش في الجرائم الافتراضية وخاصة منها المكونات المنطقية (البرامج والبرمجيات والبيانات) ورغم الجدل الفقهي إلا أن المسألة حسمت لصالح أنه يمكن إجراء التفتيش على مكونات الحاسوب سواء المادية أو المنطقية .

وللوقوف على ذلك سأتناول في **الفرع الاول** / برامج الحاسوب وفي **الفرع الثاني** / سأتناول بيانات الحاسوب.

الفرع الاول

برامج الحاسوب

COMPUTER GENERETED EVIDENCE

لقد أدى ظهور الحاسوب وارتباطه بالإنترنت إلى إثارة العديد من المسائل على الصعيد القانوني ومنها إجراءات التفتيش ومدى قابلية مكونات الحاسوب للتفتيش بنوعيها المادية والمعنوية (المنطقية). والتغير الذي حدث في النظرة القانونية للدليل والتقدير قيمته ومدى صلاحيته لإثبات الإدانة أو البراءة، إلا أن هذه المسائل حسمت وانتهى فيها الجدل القانوني إلى أن مكونات الحاسوب المادية لا تثير أي إشكاليات باعتبارها أشياء محسوسة ورغم أن المكونات المنطقية وهي البرامج والأنظمة والبيانات لا تشكل أي محتوى مادي فإن التشريعات المقارنة اعترفت بها، وأقرت بقابليتها لإجراءات التفتيش وقبولها كأدلة يمكن تقديمها للمحاكم والدفع ببطلانها في احيانٌ أخرى (1). إن أهمية محتوى الدليل الرقمي بعد الاعتراف بصحة الدعامة التي تحمله سواء أكان في العالم الرقمي أو الافتراضي ، لذلك يلزم التمييز بين الدليل الذي ينتجه الحاسوب تحديداً ويساهم في تكوينه وإنتاجه رقميا وهو ما يطلق عليه COMPUTER GENERETED EVIDENCE وهو ما يعني أن الفرد (المستخدم) لا يتدخل في تكوينه بأي طريقة وبين نوع آخر يكون الفرد مسئولا عن تكوينه وهو الدليل المخزن رقمياً COMPUTER STARED- RECORDS وعن البحث في محتوى هذا الدليل نجد أن الفرد هو من قام بتكوينه وأنشأه في البيئة الرقمية .(2) ولو تتبعنا مخرجات حركة البرامج التي يقوم بتكوينها الحاسوب فإنه يلاحظ عليها الطبيعة الرياضية الجبرية ALGORITHM فإن الذي يسيطر عليها ليس مرتكب الجريمة أو مستخدم الحاسوب وبقدر ما يكون المسيطر في

1- د.عمر محمد بن يونس – الدليل الرقمي – ط1 – منشورات الجمعية العربية لقانون الانترنت – القاهرة 2008 م-ص26

2- المرجع السابق – ص 27.

هذه الحالة هو الحاسوب ذاته (1) عند استقباله للبرمجيات التي تعمل على تشغيله وتفاعله، أما الإنترنت فإن المسيطر هو مزود الدخول لخدمات الإنترنت ISP تحديداً والذي يسمح بدخولنا إلى الإنترنت والاستفادة من خدماتها ولذلك لمعرفة زمن الدخول إلى الإنترنت لمرتكب الجريمة فإنه يتم الاستعانة بمزود الدخول للإنترنت ولا يتم اللجوء إلى حاسوب المستخدم في العادة.

إن مخرجات حركة البرامج (2) (هي مجموعة التعليمات والأوامر والإرشادات التي تظهر في شكل مربعات أو مستطيلات على الشاشة أمام المستخدم وتحمل تعليمات معينة تتعلق بنظم التشغيل للحاسوب ومثالها HISTORY والجداول الحوارية DIALOGUEBOX) وكذلك الحال في التعليمات التي تظهر أثناء فتح البريد الإلكتروني والتي تأتي في صيغة مراسلة يقوم بإعدادها الخادم المخصص للبريد الإلكتروني وليس الفرد . وكذلك البرامج التي يتم إعدادها لحركة البرمجيات في العالم الرقمي والتي تتخذ نظاماً برمجياً له طابع المجانية.

وإذا تم إجراء التفتيش الرقمي على هذه المخرجات وتحصل القائم بالتفتيش على دليل، فإنه لا يعتد به ومثالها سجل HISTORY والسبب أن المستخدم للإنترنت قد يتصفح مواقع عن طريق الخطأ ولا يطلع عليها بالكامل فيقوم الحاسوب بإنزالها ضمن المواقع التي تصفحها في السجل رغم أنه لم يطلع على أي معلومات أو يخزن أياً منها في ذاكرة الجهاز، كذلك الأخطاء التي يرتكبها نظام تشغيل الحاسوب TAMP لا تعتبر دليلاً إنما يمكن استخدامها بطريقة أمنية عند جمع المعلومات والتحريات عن موضوع معين والتأكد منه (3).

---

1. مرجع سبق ذكره – ص 28.
2. نفس المرجع السابق – ص 28.
3. د.عمر محمد بن يونس – مرجع سبق ذكره – ص 29

وفي **النوع الثاني** من الأدلة الذي يكون الفرد مسئولا عن تكوينه وإنشائه كما في حالة التخزين الإلكتروني COMPUTAR STQRED- RECORDS ويفهم من هذه العبارة أن الفرد هو الذي تدخل في تكوين الملف أو الملفات التي يتم تخزينها في الحاسوب ، والمعيار الذي يميز مخرجات حركة الحاسوب عن الملفات المخزنة هو التدخل الإنساني في تكوينها وبشكل مباشر إذ يلزم أن تتضمن حضوراً للإنسان ومثالها أقوال متضمنة في ملف معالجة الكلمات ومحتوى البريد الإلكتروني الذي يكتبه الفرد بقصد إرساله ، والعدوان الرقمي على حقوق المؤلف وهذا المثال الأكثر تداولاً عند المزج بين عمل مخرجات حركة البرامج وبين التخزين الرقمي .

وقد اشترط القانون الأمريكي صحة وأصالة الدليل الرقمي بقبوله. أما فيما يتعلق بالدليل المخزن STQRED- RECORDS فإنه يلزم ثبوت أن الدليل المستمد منه ليس شهادة سماع فهي غير مقبولة وفق النظام الأمريكي وهي استثناء وليس قاعدة (1).

1. د. عمر محمد بن يونس - مرجع سبق ذكره – ص 30

الفرع الثاني

بيانات الحاسوب

DATA

إن الحاسوب يقوم في تركيبته على ثلاثة أمور هي القطع الصلبة HARDWERE والقطع المرنة أو البرمجيات SOFWARE والبيانات DATA ذات القدرة الاستردادية على شكل معلومات ANFORMATIONSوهي موزعة بين البرمجيات والقطع الصلبة. لذلك فالحاسوب يتعامل مع منطق الحرية والتي تختلف عن الحرية الملتزمة التي يقررها القانون ، وإنما ينطلق من تعامله مع كل ما يمكن إدراجه فيه من بيانات ومهما كانت ، وهذا ما يجعلنا ندرك أن التمييز بين المشروعية واللامشروعية في الجرائم الافتراضية مبعثه قواعد القانون وليس التقنية (التكنولوجيا) (1) وغاية هذا التمييز ليست البرمجيات بل ما تحتويه من معلومات يتم استردادها سواء جاءت في شكل رسومات أو أشياء مسموعة أو شكل كتابة أو على شكل مرئي معروض ، لأن البرمجيات التي يمكن أن تحتوي بيانات غير مشروعة يمكن استخدامها (2) بطريقة كلية أو بشكل جزئي من أجل أن تعمل عليها نظم حاسوبية أخرى مشروعة وهذا هو الأصل ، ولهذا الأصل استثناء فالقانون يجرم تخزين البرمجيات التي تساهم في ارتكاب مجموعة من الجرائم كما هو الحال في نص المادة 223 في القانون العماني ، ويعتبر القرص الصلب هو البيئة التي تخزن فيها البيانات داخل الحاسوب . وعند إجراء التفتيش على البيانات داخل القرص الصلب للحاسوب ويؤدي هذا الإجراء إلى التعرف على فحوى البيانات ذات الرقمية الثنائي، وعند التعامل معها يؤدي إلى الكشف عن القيمة الاستردادية للبيانات التي تم تخزينها سواء كانت صورة أو صوتاً أو كتابة ... إلخ (3).

1- د.عمر بن يونس – الدليل الرقمي – مرجع سبق ذكره – ص 72.
2- المرجع السابق – ص 73.
3- المرجع السابق – ص 75 .

وكذلك ما تم حذفه DELETE من برمجيات وبيانات وبرامج فالأمر مرتبط ببرمجيات معينة وليس بقطع صلبة ، وكمثال على ذلك هو البحث في ملفات النسخ الإضافية التي تحتويها نظم التشغيل مثل النوافذ كملفات INTERNET TEMPORARY FILE, TEMP والأخيرة عبارة عن ملفات تأخذ نسخاً احتياطية من ذاكرة الحاسوب لكل صفحة يتم الدخول إليها عبر الإنترنت ، وهناك ملفات في نظم التشغيل خاصة بالإنزال DOWNLOUD FILE ووظيفتها استقبال الملفات التي يتم تحميلها على الحاسوب من خارجه أو عبر الموقع التي تصفحها عند استخدامه للإنترنت ، فهذه الملفات جميعها مركزها القرص الصلب حتى ولو كان هناك أماكن أخرى داخل الحاسوب تحتوي على برمجيات ومثالها PROCESSOR والذي يتم تصنيعه ووضع برمجية خاصة به في ظل ظروف خاصة للقيام بدوره داخل الحاسوب . (1).

ولأهمية البرمجيات فقد اهتم بها المشرع المقارن وأقر بأن البرمجيات المعطوبة يمكن أن تؤثر في وظيفة الحاسوب فتجعله محل شك يمكن أن يضعف قيمة البرمجيات كدليل أمام المحكمة ، بالإضافة إلى شرط سلامة الحاسوب وهو أن يكون عمل القطع الصلبة بطريقة عادية وطبيعية كما هو الحال في حاسوب آخر من ذات التركيبة , حتى يمكننا أن نتجنب رفض المحكمة الاعتداد بالدليل المستخرج منه , وفي القضاء المقارن فإن شرط سلامة الحاسوب هو محل دفع بالطعن في صحة و سلامة الدليل المتحصل عليه بحيث يجب الكشف على حركة الحاسوب والإقرار بسلامته تقنياً ، وذلك منذ قضية ROSENBARG في القضاء الأمريكي حيث قررت المحكمة قبول الدليل الرقمي إذا كان مستمداً من حاسوب سليم (2) وسوف نتناول هذه المسائل في الباب الثاني المبحث الثاني من هذه الدراسة .

والجدير بالذكر ان الفكر العربي الموسوعي المعاصر وضع حلولاً لمشكلة قواعد البيانات

1- د. عمر محمد بن يونس – الدليل الرقمي - مرجع سبق ذكره – ص 76.

2- المرجع السابق – ص 81.

ولعل أبرز مظاهرها على الإطلاق موسوعة التشريعات العربية التي تعتبر بحق أكبر (1) قاعدة بيانات تشريعية في العالم والتي وضعها المواطن الليبي الأستاذ المرحوم / محمد أبوبكر بن يونس (1932 م- 2001 م) مما جعلها تتفاعل مع العالم الافتراضي وتكنولوجيا المعلومات (2).

حيث قام قسم الأبحاث بخطوات تقنية من أجل أن تكون هذه القاعدة الضخمة للبيانات DATA في ملفات صغيرة الحجم وبالتالي يمكن تقديمها في أقراص ومن ناحية أخرى تم الشروع في إعداد الشبكة القانونية العربية على موقع

http//www.alen.com والتي اعتمدتها الجامعة العربية (3) حتى يمكن أن يحدث تواصل بين فكر صاحب موسوعة التشريعات العربية وبين العالم الرقمي حيث تم اعداد موضوعاتها بكفاءة عالية نالت إعجاب القانونيين في العالم.

1- د.عمر محمد بن يونس – مشكلة قواعد البيانات – ط1 دار الفكر الجامعي – الاسكندرية 2004 م – ص 12.

2- سجلت موسوعة التشريعات العربية في سجل جينيس للأرقام القياسية – 1999- كتاب 2002 م –ص 156.

3- بداء البث التجريبي للشبكة القانونية العربية في 1997/12/24م .

الفرع الثاني

إذن التفتيش الرقمي الممتد وآثاره

يهدف التفتيش إلى الحصول على الأدلة سواء في منزل المتهم أو بحوزته أو في أي مكان ترك نشاطا يمكن معرفته والاستدلال عنه ومحل التفتيش في جرائم الإنترنت هو العالم الافتراضي، وإجراء التفتيش يستتبع بالضرورة ضبط الأشياء وتحديد الأدلة المستمدة من التفتيش تعد من المسائل المهمة في الجرائم المرتكبة عبر الإنترنت لكون الدليل المستمد منها ذا طبيعة رقمية وتستلزم إجراءات التحفظ عليه قواعد خاصة يجب أن يلتزم بها القائم بالتفتيش. (1).

ويعد التفتيش الذي يجريه مأمور الضبط القضائي من الصلاحيات الاستثنائية التي منحها له القانون طالما قامت مبرراته دون الرجوع لسلطة التحقيق لمنحها الإذن بإجراء التفتيش وهي حالات محددة .وتشمل حالات التلبس بالجرائم والقبض والجرائم التي تكتشف عرضا من تفتيش صحيح ، باعتبارها حالة تلبس وقد جاء نص المادة (36) أ-ج ليبي على الاتي" لمأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن يفتش منزل المتهم ويضبط فيه الأشياء والأوراق التي تفيد في كشف الحقيقة إذا اتضح له من أمارات قوية أنها موجودة فيه " (2) وهذا النص يجيز تفتيش محتويات المنزل المختلفة بما فيها الحاسوب وحيثما وجد ، ما دام داخل منزل المتهم وفي نص المادة (35) أ-ج ليبي أنه " في الأحوال التي يجوز فيها القبض قانونا على المتهم يجوز لمأمور الضبط القضائي أن يفتشه " (3) ، وهذا النص يفيد بإمكانية تفتيش الحاسوب النقال الذي بحوزة المتهم المقبوض عليه وبالتالي يشمل ذلك الامتداد في تفسير النص كذلك هاتفه النقال إذا كان الحاسوب جزءاً من عمله أما **الحالة الثالثة** فقد وردت في نص المادة (39)أ-ج ليبي على أنه " لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع

1- د. عمر محمد بن يونس - الجرائم الناشئة من استخدام الإنترنت – ط 1 – دار النهضة العربية – القاهرة 2004 مرجع سبق ذكره صـ855.

2- مجموعة التشريعات الجنائية – ج 2 -الإجراءات الجنائية – الإدارة العامة للقانون -1987 م

3- نفس المرجع السابق.

الاستدلالات أو حصول التحقيق بشأنها ، ومع ذلك إذا ظهر عرضاً أثناء التفتيش وجود أشـــياء تعد حيازتها جريمة أو تفيد في كشـــف الحقيقة في جريمة أخرى جاز لمأمور الضبط القضائـــي أن يضبطها " (1) وهذا النص يتناول مسألة التفتيش العرضي والتي تجيز لمأمور الضبط القضائي اكتشاف وضبط جريمة أخرى لم تكن إجراءات التفتيش تهدف إليها ، وبالتالي يتكون اتهام جديد وهو يفترض وجوده بكثرة في جرائم الإنترنت فيما يعرف بالجريمة العرضـــية ومثالها قيام مأمور الضـــبط القضـــائي بتفتيش جهاز الحاسـوب الشـخصـي لإحدى الهكرة وأثناء ذلك يجد أمامه صـورة إباحية مخزنة مما يعني وجود جريمة أخرى (2) وفي حالة القبض على الأشـخاص وجواز تفتيشـهم وما يحملونه من أمتعة أو حقائب أو أغراض شخصية فإن معنى امتداد التفتيش أثناء القبض على الأشـخاص يمكن تصـوره ، فعند وجود مبرر للقبض على المتهم يجوز تفتيشـه قانونا وهو ما يتطلب بالطبع تفتيش حاسوبه النقال وهاتفه وكل ما يحمله من وسائط قد تحتوي على أدلة رقمية وهذه المسائل لا تحتاج إلى إذن من سلطة التحقيق (3) . أما في حالة تفتيش منازل المتهمين وهي الحالة العادية وليسـت الاسـتثنائية فإن القواعد العامة تتطلب وجود مبررات لمنح الإذن بتفتيش المنزل أو المكتب وما يمكن أن يحويه من أدلة بالتخصـيص مثل الحاسـبات أو الملقمات أو المضـيفات أو البيانات والمعلومات المخزنة في الحاسـوب المنفرد وهذه القواعد تتعلق بمحتويات المنزل أو المكتب أو المؤسـسـة وعلاقتها بالأدلة الرقمية والتي لها علاقة بالجريمة الجاري التحقيق فيها أما القواعد التي تتعلق بضـرورة تحديد مكان التفتيش تحديدا نافيا للجهالة وبناء على ذلك فيجب أن تكون التحريات جدية من قبل مأمور الضبط القضائي في هذا المكان بالتحديد الدقيق بالاسم والرقم والشارع ... إلخ .

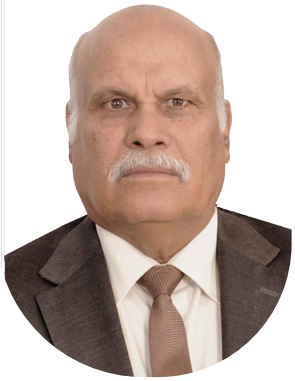
1- مجموعة التشريعات – مرجع سبق ذكره.
2- د.عمر بن يونس – مرجع سبق ذكره – ص 859
3- المرجع السابق .ص 860

وبالتالي يمنح مأمور الضـبط القضـائي إذن التفتيش بناء على التقيد بهذه القواعد وهذا يعني أنه لا يجوز له إجراء التفتيش أو القيام به إلا في المكان والزمن المحددين من قبل سلطة التحقيق، وهذه المسألة لا تثير أي إشكاليات عن تفتيش الحاسوب المنفرد، أما إذا كان التفتيش يهدف إلى الانتقال المادي بين الخوادم فسـوف نكون أمام تغير في الأماكن التي ينطلق منها النشـاط التقني وبالتالي طبقا للقواعد العامة فهي تحتاج إلى إذن تفتيش لكل الأماكن والمواقع المراد إجراء التفتيش عليها عند تتبع مسـار حركة الإنترنت، إن سـبب امتداد إجراء التفتيش هو وجود Trace أي الأثر وكمثال على ذلك إذا تحصـل مأمور الضـبط القضـائي على إذن تفتيش في جريمة جاري التحقيق فيها بعد اتخاذه الإجراءات الأولية وانتقل إلى خادم الشـركة server وأثناء التفتيش تبين أن أثر الهاكر انطلق من خادم جامعة طرابلس وتم الانتقال إلى خادم جامعة طرابلس وعند البحث عن Trace تبين أنه استخدم حاسوب موجود بكلية الطب البشري وبالانتقال إلى كلية الطب البشـري وبتفتيش الخادم تبين أن الدخول تم من منزله وبمعرفة ip تم التعرف على البيانات الشخصية لصاحب الجهاز (الاسم وعنوان المنزل) وبالانتقال إلى منزل المتهم وتفتيش حاسوبه الشخصي تبين أنها نقطة الانطلاق الأولي للنشاط التقني .

إن الخوادم الموجودة في أماكن مختلفة ، ولما لحالة الاسـتعجال في تتبع مسـار حركة الإنترنت حيث تتطلب إجراءات سريعة وفورية لضبط الجناة وخاصة إذا كانت الجرائم المرتكبة تهدد أمن وكيان الدولة أو متعلقة بالإرهاب أو دعم الإرهاب أو عمليات غسـل الأموال ، أو مكـافحـة الجرائم عبر الإنترنـت أو مكـافحـة جرائم الإرهـاب الإلكتروني ووضـعت برامج تقصـي ومراقبة عبر الإنترنت مثل برنامج كارنيفور متطور من قبل المصـالح العليا للدولة رغم ما سـوف يثار من مسـائل تتعلق بحقوق الإنسـان وقوانين الخصـوصـية التي تحرص معظم التشـريعات الغربية والعربية على الاهتمام بها وتضمنها لنصوص قوانينها .

وإذا لاحظنا نصـــوص مشـــروع قانون الجرائم الافتراضـــية المقترح من موســـوعة التشريعـــــات العربية نجد أثر رأي الفقيه (أورين كير) واضحا في نص المادة (82) على أنه " يكتفى بإذن تفتيش واحد إذا كان هناك دلالة تســـتدعي تتبع مســـار الجريمة بالانتقال المادي بين الخوادم في أماكن مختلفة ولا تســـري هذه المادة إذا كان بين هذه الأماكن حواســيب أو خوادم في مســاكن خاصــة ويراعي مبدأ التعاون الدولي والثنائي والإنابة القضـــائية في إطار التفتيش خارج الحدود الليبية إذا كان لذلك حاجة " (1) ، ونحن نرى أن سـيادة هذا المبدأ سـوف يكون لها صـدى واهتمام من قبل فقهاء وعلماء القانون على المسـتوى العالمي . وتسـتلزم أغلب التشـريعات الإجرائية حضـور بعض الأشـخاص لإجراءات التفتيش وذلك كضـمانة لصـحة الإجراءات من الناحية الشـكلية. وهو ما سنعرض له في **الفرع الثالث** من هذا المطلب.

1--مشروع قانون الجريمة الافتراضية والدليل الرقمي (مقترح من موسوعة التشريعات العربية)



إعداد :
فرج بشير برنوص
ماجستير قانون جنائي (فرع قانون الانترنت)
خبير محلف فى الجرائم الافتراضية 2017م

عِلم الضحية عبر الإنترنت

مُقدّم للدورة الأولى للمستشار الأمني لضباط جهاز المباحث الجنائية
المنعقدة بجامعة العاصمة للعلوم الإنسانية والتطبيقية

مقدمة

منذ زمن ليس ببعيد بدأت مصطلحات العالم الافتراضي تفرض نفسها على المجتمع القانوني العربي بالتحديد، ولاحظ الباحثين والدارسين في المجال القانوني هذه المصطلحات فتناولوا البعض منها بالدراسة والبحث العميقين، والبعض الأخر تناولها على سبيل عرض الموضوع للبحث في المجال القانوني وترك الباب البحثي مفتوحاً للجميع، وهناك مصطلحات لم تطرق بعد ولكنها في أفكار وعقول بعضنا نحن المهتمين بهذا المجال،

ولذلك كان نتيجة لتوجيهات سعادة **الدكتور / عمر محمد يونس** لنا، نحن كفريق خبراء قانون الإنترنت في ليبيا الأثر الكبير في شد انتباهنا للعديد من الموضوعات الجديرة بالاهتمام والتي منها موضوع (علم الضحية عبر الإنترنت)، ولا نقصد المفهوم العام للضحية في كتب علم الإجرام أو ضحايا الإجرام، بل تعني أن الأهداف المعرضة للجرائم الافتراضية هي في حقيقتها ضحايا، سواء كانت شخصاً طبيعياً أو اعتبارياً، بسبب أن هذه المؤسسات والشركات والهيئات تمتلك المعلومة، وهي أهم المصالح المحمية جنائياً إذ كان القانون يترتب علي الاعتداء عليها جزءاً جنائياً .

وعلى الرغـــم من أن المهمة الرئيسية التي يضطلع بها النظـــام الجنائي الموضوعي (قانون العقوبات العام)، والإجرائي (قانون الإجراءات الجنائية) وكامل الأجهزة التنفيذية التي تسهر على تطبيقه، لمواجهة الظاهرة الإجرامية للحد منها، ومع ذلك فإنه ما يزال قاصراً على تحقيق هذه المهمة بسبب التحديات التي ظهرت بظهور التقنية ومزاياها المتعددة، ومن محاسن الأبحاث والدراسات القانونية الجنائية أنها تكشف عن مناحي هذا القصور، وتضع الحلول الناجحة وتطويع التشريعات لمواجهة الظواهر الإجرامية المستحدثة.

ولا مشاحة في أن دراسات علم الضحية اهتمت في البداية بدور الضحية في الجريمة، إلا أنها في مرحلة لاحقة اتجهت إلي بحث حقوق الضحية في النظام الجنائي، وعلى الرغم من أنها قد تكون طرفاً رئيسياً في الجريمة بحيث يمكن أن يكون لها دور في وقوعها، فإنه مع ذلك يلحق بها ضرر وتنتهك حقوقها من جرائمها، لذلك من المفيد لنا أن نهتم بحقوق الضحية التي أهدرتها الجريمة.

مشكلة البحث: -

- بتقدم التقنية واندماجها مع الاقتصاد ظهرت مصطلحات لم تكن معروفة ابرزتها تطورت العالم الافتراضي ومنها مصطلح الاقتصاد الرقمي. تطلب بذلك أن تعمل كبرى الشركات التقنية على الاستفادة من هذا الوضع، بطريقتها لاستثمار البيانات المخزنة على خوادمها بعلم المستخدمين أو بدون علمهم، وظهور مؤسسات وشركات أخرى تعمل في مجال المعلومات وبيعها للاستفادة منها في الدراسات والأبحاث على شعوب العالم. فهل تصبح هذه البيانات الموجودة على خوادم كل الشركات ضحية (مجني عليه) في مجال التقنية باعتبارها تعرضت للاعتداء، وهذه الإشكالية التقنية والقانونية التي سيتعرض لها بحثنا.

أهمية موضوع البحث: -

- تتجلى أهمية موضوع البحث في قيمة تلك البيانات التي تتحل إلى معلومات وما تحمله من قيمة اقتصادية وخصوصاً إذا عدت بالتريليونات دولار ومن مختلف دول العالم، وحاجة الدول للدراسات والأبحاث الاستراتيجية والعسكرية والتنموية عن شعوب بعض الدول وصراع الأقطاب الكبرى في العالم، فالدول تعي جيداً أهمية المعلومات ودورها في الاقتصاد والتقنية بالإضافة إلى العوائد المالية الناتجة عن استغلال هذه المعلومات، فهل تصبح هذه المعلومات ضحية كما هي في العالم المادي المعروف لدينا؟

أهداف البحث: -

يهدف البحث إلى الإجابة عن بعض الأسئلة التي تدور في خلدنا، وتحتاج إلى إجابة فمتى يصبح الشخص الطبيعي أو المعنوي ضحية؟ وهل للشخص الرقمي نفس المركز القانوني للشخص الطبيعي؟ وما هو مفهومه وطبيعته القانونية؟ وإلى أي مدى يصبح العدوان على المصالح المحمية جنائياً قوياً بحيث ينتج عنه مفهوم الضحية؟ وهل تصبح المعلومات كقيم اقتصادية ضحية؟ وهل تصبح الضحية بمفهومها الجنائي حدثاً واقعياً عبر العالم الافتراضي؟ وهل تفرض نفسها على النظام الجنائي التقليدي؟ سنحاول الإجابة عن هذه التساؤلات.

نطاق البحث: -

أن العالم الافتراضي لم يأخذ نصيبة من البحث والدراسة لحداثة مصطلحات هذا العالم، ولكون التقنية متطورة باستمرار وعلينا أن نلحق بها، فأن عنايتنا في هذا البحث ستكون مركزة على دراسة مفهوم الضحية والقيمة الاقتصادية للمعلومات، ونتائج اعتبار قيمة تقنية المعلومات أصولاً مالية والحماية الجنائية للمعلومات كقيمة اقتصادية عبر الانترنت حسب القوانين المقارنة والتشريعات الليبية.

منهج البحث: -

لقد اتبعت في تناول هذا الموضوع، المنهج التحليلي المقارن في دراسة تحليلية سيراً على منهجية مدرسة التنظيم القانوني للعالم الافتراضي (Cyber law) السائدة الآن. ولذلك جاءت **خطة البحث على التالي: -**

المبحث الأول / الضحية والقيمة الاقتصادية للمعلومات

المطلب الأول / مفهوم الضحية

المطلب الثاني / القيمة الاقتصادية للمعلومات وتحولها الضحية

المبحث الثاني / نتائج الحماية الجنائية للمعلومات وموقف القانون المقارن

المطلب الأول / نتائج اعتبار قيمة تقنية المعلومات أصولاً مالية

المطلب الثاني / الحماية الجنائية لمعلومات كقيم اقتصادية عبر الانترنت فى القانون المقارن

المبحث الأول
الضحية والقيمة الاقتصادية للمعلومات

تمهيد وتقسيم /
كانت الدراسات والأبحاث حول الجاني والضحية والتي فى حقيقتها فتحت أفاق جديدة فى الاهتمام بدور الضحية ومفهومها القانوني. لذلك وهل هناك قيم يمكن أن تصبح ضحية وفقاً للمفهوم المادي؟ وهل تشكل الضحية عبر الانترنت قيمة اقتصادية وتتحول إلى مفهوم الضحية المعتدى عليها.
كل ذلك جاء في **مطلبين الأول** / مفهوم علم الضحية **والمطلب الثاني** / القيمة الاقتصادية وتحولها لضحية عبر الانترنت.

المطلب الأول
مفهوم علم الضحية

حتى وقت قريب لم يكن معروفاً مصطلح الضحية، بل أن القانون الليبي يخلو من هذا المصطلح، ويستعمل ألفاظاً أخري تستوعب جانباً أو أكثر من الجوانب التي ينصرف إليها مدلول كلا منها ولا تستغرقها، فالمشرع الليبي أستخدم تعبيري (المضرور من الجريمة) و (المجني عليه) وفي الحقيقة، أن في الغالب تجتمع في شخص واحد صفة المجني عليه والمضرور من الجريمة، إلا أن هذه الصفة قد تنفك في بعض الحالات والوقائع، فمن الجائز إلا يلحق المجني عليه ضرر، ومن الجائز أن ينال الضرر غيره.
ولقد جاء في الإعلان الدولي بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها 34/ 40 الصادر في 29 /11/ 1985م، حيث نص على انصراف مصطلح الضحية إلى كل من المجني عليه والمضرور من الجريمة (فقرة أ- البنود 1- 2 - 3).
ومع ذلك هناك اختلاف بين مصطلح المجني عليه والمضرور، فالأول هو صاحب الحق الذي وقعت عليه الجريمة فأهدرته أو انتقصت منه أو هددته بالخطر، أما الثاني فهو كل شخص ألحقت به الجريمة ضرراً وليس شرطاً أن يكون المجني عليه، فالمعيار في ثبوت صفة المجني عليه هو كونه صاحب الحق الذي تحميه القاعدة الجنائية، والذي أعتدي عليه الجاني بارتكابه الجريمة، ولا عبرة في ثبوت هذه الصفة بمدى وقوع الضرر، أما صفة المضرور من الجريمة فالضرر هو وحدة المعيار في ثبوتها أو انتفائها، فكل من أصابته الجريمة بضرر تثبت له هذه الصفة ولو لم يكن مجنياً عليه، وبالمقابل فإن أي شخص لم ينله من الجريمة ضرر لا تثبت له صفة المضرور ولو كان مجنياً عليه .
وهذا الاختلاف في المصطلحين له أثار قانونية لها علاقة بالصفة التي تخول صاحبها مباشرة الحقوق المقررة له قانوناً، فمن حق الادعاء المباشر وحق الادعاء بالحق المدني أمام المحكمة الجنائية مقرران للمضرور من الجريمة، وبالتالي فإن المجني عليه لا يملك هذين الحقين إذا لم تصيبه الجريمة بضرر، وبالمقابل فإن حق الشكوى مخول للمجني عليه ولو لم يلحقه من الجريمة ضرر، أما غيره فليس له حق تقديم الشكوى عن الجريمة ولو تثبت له صفة المضرور من الجريمة.

وتاريخياً فإن الفضل في بدء الباحثين لدراسة شخصية الضحية يعود إلى العالم (**هينتج**) الذي يعتبر رائد علم الضحية بدراسته التي نشرها عام 1948م، وكذلك الطبيب النفسي الأمريكي (**فرديدك ويرثام**) وكانت الدراسة حول الجاني وضحيته والتي في حقيقتها فتحت أفاقاً جديدة في مجال الاهتمام بدور الضحية في الجريمة وكانت إيذانا بدخول العلوم الجنائية مرحلة جديدة برزت معالمها من خلال الندوات والمؤتمرات العلمية التي عقدت لمناقشة هذه المسألة.

ومن بين أهم رواد المدرسة العلمية للضحية الدكتور (**عزت عبدالفتاح**) وهو أستاذ مصري بالجامعات الكندية، فقد نشر في الفترة ما بين عامي (**1965 - 1991م**) أكثر من عشرين بحثاً، تدور حول دور الضحية في الجريمة، والعوامل التي تؤدي إلي وقوع الشخص ضحية، ومدى مسؤولية الضحية عن مساهمته في الجريمة، والمشاكل التي يطرحها علم الضحية علي صعيد نظام العدالة الجنائية،

وكان من بين رواد علم الضحية علي المستوى الدولي: (**هينتج، ومندلسون مارجري، وعزت عبد الفتاح، ودرابكن، وستيفن شيفر، وميازاوا**) .

ولقد نال هذا العلم اهتمام الباحثين والدارسين في مجال علم الإجرام، ولقد ورد في قاموس علم النفس أن علم الضحية هو : (العلم الذي يعني بدراسة شخصية الأفراد، ضحية جنحة أو إجرام ومراكزهم الاجتماعية وعلاقاتهم العاطفية بالمعتدي) ولقد عرفة (**فيانون VIANON**) علي أنه (العلم الذي يدرس الجرائم وكل ما يرتبط بها) ويري (**شافار SHAFERE**) أن علم الضحايا (يدرس العلاقات القائمة بين الضحية والمجرم) وفي تعريف أخر لعلم الضحية أنه : (نوع من علم الإجرام الذي يدرس الضحايا وجوانبها النفسية قبل وأثناء وبعد الفعل الإجرامي).

الفرع الأول
تصنيف الضحايا

هناك عدة تصنيفات ظهرت من خلال الدراسات والأبحاث للضحية وقد تباينت وجهات النظر وأهمها:/

- أولاً / التصنيف القائم على مدى قابلية الشخص لصفة فيه للوقوع ضحية :/

1. صغير السن.
2. الكهل.
3. الأنثى.
4. المريض وضعيف العقل.

كما يميز من الضحايا تبعاً لخصائصهم النفسية وهم:

1. المكتئب.
2. الجشع.
3. المنعزل.

ثم طورت الدراسات هذا التصنيف ومن بينهم العالم **(البنبوجر)** الذي قسم الضحايا إلى ثلاثة فئات هي: -

1. الضحية المستتر.
2. الجاني الضحية.
3. الضحية ذو العلاقة بالجاني.

ثانياً / التصنيف القائم على دور الضحية في الجريمة وهم: -

1. الضحية الحريص.
2. الضحية المهمل أو المسهل للجريمة.
3. الضحية الداعي.
4. الضحية المستفز.
5. الضحية الراضي.
6. الضحية المحرض.
7. الضحية الوهمي.

ثالثاً / التصنيف القائم على مدى مسئولية الضحية عن الجريمة ودرجة أذنابهم فيها وهم: -

1. الضحية المسئول كلياً عن الجريمة.
2. الضحية الذي يستوي مع الجاني في درجة مسئوليته عن الجريمة.
3. الضحية المسئول جزئياً عن الجريمة.
4. الضحية البريء.

ولقد أثارت مشكلة ضحايا الإجرام اهتمام بعض المفكرين، وبدأ الاتجاه نحو تحسين وضع الضحية، والاهتمام بحقوقه والدعوة التي تحمل الدولة عبأ تعويض الضحية، وظهور حركة الدفاع عن حقوق الضحايا، ومساعدتهم وذلك من خلال المؤتمرات الدولية التي اهتمت بهذا الجانب.

الفرع الثاني
الضحية عبر الإنترنت

أن الجرائم المرتكبة عبر الإنترنت، لا تقل خطورة وأهمية عن الجرائم المرتكبة في العالم التقليدي، من حيث حجم الضرر بالأشخاص والأموال، بل أن حجم الضرر في الأولي اقتصاديا لا يقارن بالثانية، وهذا الضرر قد يكون ماسا بالمصالح الشخصية، وخصوصيتهم الفردية أو بمصالحهم الاقتصادية، سواءً علي المستوي الفردي كأفراد، أو علي مستوي مؤسسات اقتصادية كبرى، والمتواجدون في العالم الافتراضي الواسع، وهذا يعني أن الضرر يخلق الضحية، مع فارق أن الضحية في العالم الافتراضي قد لا توجد علاقة مباشرة بينه وبين الجاني، بسبب ما وفرته التقنية الحديثة من وسائط التواصل، والتطبيقات بين الأشخاص في مختلف بقاع الأرض، دون حدود جغرافية فاصلة، مع ملاحظة أن بعض المجتمعات الافتراضية هي مغلقة، وليست مفتوحة العضوية، بل يتلقى المستخدم دعوة أو تزكية من أحد الأعضاء، لكي يصبح عضو جديد فيها، ومثالها

مجاميع مشاركة الملفات التي تستخدم تقنيات التشفير لإخفاء أنشطتها الداخلية، وكذلك أنشطة الإنترنت السفلي الديب ويب **(deep web)** .

وبالرجوع إلى خصائص الجرائم الافتراضية نجد أن أحجام الضحية عن الإبلاغ عن الجريمة سواء على المستوي الشخصي أو على مستوي المؤسسات الاقتصادية والمالية الكبرى، بسبب الخوف من المكانة الاقتصادية في السوق وفقدان الثقة للعملاء في هذه المؤسسات، حيث تبين من الدراسات والأبحاث أن ثلث الضحايا في العالم الافتراضي هم الذين يتقدمون بالشكاوى للشرطة فقط.

المطلب الثاني
القيمة الاقتصادية وتحولها لضحية

تُعتبر الإنترنت من أهم الوسائل المعاصرة التي تساهم وبشكل كبير في تعميم المعرفة، ونشرها وأهم وسيلة لتبادل الخبرات، والمعارف والمعلومات، ونشر الثقافات المختلفة بين مستخدميها، ومد جسور التواصل والصداقة، بين سكان الأرض دون اعتبار للحدود الدولية الفاصلة بين دول العالم كما عرّفها أستاذنا الفاضل الدكتور /عمر محمد بن يونس خبير جرائم الانترنت.

وبسبب الخصائص التي تميز العالم الافتراضي، وسهولة الوصول للمعلومات المختلفة وتعرضها للعدوان، لأهداف مختلفة التي برزت في السنوات الأخيرة ومثالها الإرهاب الذي طال معظم دول العالم، وفي هذا الجانب قالت رئيسة وزراء بريطانيا **(تيريزا ماي)** : أنها ستغير قوانين حقوق الإنسان إذ كانت تعترض طريق التعامل مع المشتبه في كونهم إرهابيين، وقالت أيضاً ... وبعد هجوم لندن (أن الأشياء يجب أن تتغير في مجال مكافحة الإرهاب، ولا يمكن السماح لهذا الفكر، و نحتاج لقواعد جديدة للفضاء الإلكتروني)، و كذلك في فرنسا صرح الرئيس الفرنسي **(ايمانويل ماكرون) :** أن فرنسا ستحارب الإرهاب داخل وخارج أرضيها، وأنها ستكون في الصف الأول لمواجهة الإرهاب .

ولقد أصبحت المعلومات من أهم الأسس التي يقوم عليها تقدم الأمم والشعوب، لأنها المادة الخام للبحث العلمي والقاعدة السليمة لاتخاذ القرارات الصحيحة، بل أن من يملك المعلومات المناسبة وفي الوقت المناسب، فإنه يملك عناصر السيطرة والقوة في عالم يعتمد علي العلم في كل مناحي الحياة.

ولذلك تتوقف قيمة المعلومات في معظم الأحيان على قدر أهميتها وحجمها وحداثتها بالنسبة للمستفيد منها، فالأمم تستخدم المعلومات والمعرفة على اعتبارها قيم اقتصادية واستراتيجية بل ومن ضمن أمنها القومي.

الفرع الأول
مفهوم المعلومات وقيتهما

علي الرغم من أن مصطلح المعلومات يستخدم في حياتنا اليومية وبشكل واسع، إلا أنه توجد صعوبة في تحديد دقيق ومتفق عليه لهذا المصطلح، وتوجد له عدة تعريفات نذكر منها علي سبيل المثال، وفقاً لتعريف المعجم الموسوعي لمصطلحات المكتبات والمعلومات بأنها (البيانات التي تمت معالجتها لتحقيق هدف معين، أو لاستعمال محدد لأغراض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها أو تفسيرها أو تجميعها في شكل ذي معنى) ويعرفها **(ديفيس واولون)** بأنها (بيانات تمت معالجتها وتحويلها إلي صيغة

مفيدة، ذات معني بالنسبة إلي المستخدم، ولها قيمة حقيقية أو متصورة في الأفعال أو القرارات الحالية أو المحتملة) .

الفرع الثاني
مفهوم القيمة

حتى يمكننا وضع تعريف محدد وواضح للقيمة، فإن ذلك يتطلب منا مراعاة المراتب السبعة، التي وصفها الفيلسوف **(أرسطو)**، قبل أكثر من ألفي سنة، والتي تعتبر الإطار العام الذي من خلاله تحدد الصورة الكلية لقيمة الشيء، وهذه المراتب هي:

1. الاقتصادية.
2. السياسية.
3. الاجتماعية.
4. الجمالية.
5. الأخلاقية.
6. الدينية.
7. الشرعية.

ولقد حضيت المرتبة الاقتصادية بالاهتمام والدراسة والبحث بشكل أكبر، لأنها أنصبت على القيمة الاقتصادية التي تم تقسيمها إلى أربعة أنواع متداخلة مع بعضها، وهي قيمة الكلفة وقيمة التبادل وقيمة التثمين وقيمة الاستخدام، ويؤذي هذا التداخل إلى أن أحد الأنواع قد يؤثر في الأنواع الأخرى بنسب متفاوتة، أو قد تشترك أكثر من واحدة في التأثير، وكمثال: قيمة التثمين وقيمة الاستخدام يمكن أن تأثر معاً على قيمة التبادل.

الفرع الثالث
قيمة المعلومات الاقتصادية

يلاحظ عدم الاتفاق علي تعريف واضح و ثابت لهذا المفهوم، لأنه مفهوم متعدد الأبعاد، وهناك عدة تعريفات منها : (أن قيمة المعلومات زيادة قناعة مستخدمي المعلومات، بالمعلومات المستحدثة) ويري تعريف أخر بأن قيمة المعلومات هي : (صلة المستخدم بالمعلومات، وما تتضمنه تلك المعلومات من قيم إخبارية لذلك المستخدم)، ولقد وضع **هيلتون (Hilton)** ثلاثة تعاريف لقيمة المعلومات، عبر عنها بثلاث معادلات بصيغة كمية الأولى، تجد قيمة المعلومات من خلال وحدات المنفعة المتحققة، وقيم العرض والطلب نجد قيمة المعلومات، من خلال الزيادة في المنفعة المتوقعة، الناتجة من الانتفاع من المعلومات، وتحدد الثانية قيمة المعلومات من خلال قيمة الطلب للمعلومات، والتي تمثل الكميات القصوى المقاسة بالوحدات، وتحدد الثالثة قيمة العرض للمعلومات، ندرة هذه المعلومات، وأصول تكنولوجيا المعلومات التي يمكن أن تعد قيمة

مالية، هي القيم التي تصلح أن يدخل في الحركة المالية في سوق العمل، وبالتالي تصلح أن تكون نشاطاً مستندياً ومحاسبياً للمؤسسات والشركات، مثل السندات وغيرها، ويعد مدخل للقيمة الاقتصادية للمعلومات، أحد أهم الجوانب المهمة في المعلومات، وتعتمد قيمة المعلومات عند احتسابها على نتيجة القرار، أو على النتيجة المتوقعة، إذ لا يمكن تميز المعلومات قبل استخدامها، فالاستخدام، أو مجالات الاستخدام، والمستفيدون، هو الذي يمنحها القيمة الاقتصادية من خلال الحصة السوقية، أو أسواق المنافسة الاقتصادية، وخاصة في عالم التقنية المتطور وبشكل سريع، فالجهة التي تقدر قيمة المعلومات اقتصادياً هي الجهة المالكة لهذه المعلومات، وخصوصاً إذا كانت محتكرة لهذه المعلومات.

ولذلك تحرص الشركات والمؤسسات الكبرى في عالم التقنية على المحافظة علي سرية هذه المعلومات، وحمايتها بكل الوسائل المتاحة لديها، وتعمل على تطوير وتحديث برامج الحماية من حين لأخر، وفي جانب احتكار المعلومات، بدأ **(ريتشارد ستالمان)** مشروع **جنو** سنة **1983م** لبناء نظام تشغيل حر بالكامل، يوفر لمستخدمي الحاسوب حريتهم، ويعفيهم من اللجوء لاستخدام برمجيات محتكرة، تسلبهم حريتهم في تعديل وتطوير مشاركة البرمجيات مع بعضهم البعض.

ولقد ضم مشروع النواة **لينكس**، إلى مشروع **جنو**، وأطلق عليه **(جنو لينكس)**، بحيث أصبح نظام تشغيل متكامل، وكان بفضل أبرز أعضائه **(ريتشاد ستالمان)**، والذي تم تطويره خلال السنوات الماضية، وهو من البرمجيات الحرة، وأصبح يعمل على العديد من المنصات من الخوادم العملاقة، إلى الحواسيب المنزلية، وأجهزة الهواتف الجوال.

وتطورت واجهات المستخدم العاملة عليه لتدعم كل لغات العالم تقريباً، وبسبب كونه حر (مفتوح المصدر)، وسهوله تطويره وإتاحة ذلك للجميع، فإن سرعة تطوره عالية، وأعداد مستخدميه تتزايد على مستوي الأجهزة الشخصية، والخوادم ومن أهم موارد المعلومات، هي البيانات **(Data)** حيث أنها المورد الأول والخام للبيئة المعلوماتية، وهي المدخلات المباشرة التي تغذي منظومتها المعرفية، والثانية المعلومات (information) وهي مجموعة البيانات بحالتها الخام، التي تمر خلال مرحلة أو مراحل من المعالجة، لتصبح على هيئة قواعد بيانات.

وللتحديد الدقيق كقيمة المعلومات الاقتصادية، تعتبر وحدة العملة النقدية أوضح مقياس لعنصر القيمة الكامنة في أي معلومة، وكلما زاد أثر هذه القيمة في النشاط الاقتصادي أو العلمي أو العسكري، ازدادت أهميتها، وبالتالي قيمتها الاقتصادية، وتوجد أنواعاً أخري من المعلومات، مثل معلومات الإعلان و الأفكار السياسية، التي تزداد قيمتها كلما صارت أكثر انتشاراً، وتنجح في اختراق زوايا البيئة التي تطلق فيها، وستكون قيمتها في هذه الحالة ناجحة في تأثيرها علي الأفعال، مثل تشجيع الإقبال علي الشراء، أو قرارات التصويت أو الانتخاب، أو المنافسة العسكرية.

وقد اقترحت الدراسات والأبحاث عدة عناصر جوهرية لتحديد القيمة، منها عنصر التطوير وعنصر العمليات وعنصر السوق وأخيرا عنصر التجميل، إلا انه يجب ملاحظة وجود صعوبة في تحديد القيمة الاقتصادية للمعلومات بدقة، ولذلك من المنطقي أن نعتبر أن الانترنت هي مجال واسع للتجارة بكل أنواعها، ومميزاتها التي وفرتها وسائل الاتصال بالإنترنت، وبالتالي يمكن اعتبارها احتياطي استراتيجي للدولة، ولقد أقرت أحدي المحاكم الأمريكية مبدأ قضائي ينص علي أن : (الإنترنت هي منطقة تجارة ، ويجب أن يتم

معاملتها كاحتياطي وطني، لكي يمكن حماية المستخدم من التنظيم غير الدقيق لها، والذي يمكن أن يصل بها إلي الشكل التام، الذي يتسبب في تخلف تطويرها، و أن أي تنظيم غير قانوني لطريقة الاستخدام الغير المشروع للإنترنت ينتهك شرط التجارة الدستوري) .

الفرع الرابع
المعلومات التي تتحول إلى ضحية عبر الانترنت

تشكل قواعد البيانات في العالم الافتراضي، أو في جانب التخزين الرقمي للبيانات غير المرتبطة بالإنترنت، حجم كبير من البيانات، وتتحول إلى معلومات ذات قيمة اقتصادية عالية، تختلف باختلاف الجهات المالكة، ومحتوى هذه المعلومات ومدي الإقبال عليه، وبالتالي تحولها إلى ضحية، ويمكننا أن نحدد أهم الأهداف المعرضة للعدوان من المخترقين (الهاكر)، بسبب المعلومات وقيمتها الاقتصادية، ويمكن أن توجد قيم تكنولوجيا المعلومات في القطاع الخاص ومثالها:

أولا // شركات محركات البحث ومنها:

1. التافيستا (aitavista)
2. جوجل (coogle)
3. أية أوال (aol)
4. هوت بوت (hot bot)
5. لايكوس (ly cos)
6. بينغ (bing) وهو تصميم مايكروسوفت
7. ياهو (yahoo)
8. بايدو (bai de)
9. ولفرا مالفا (wolfro malpha)
10. داكد كوغو (dackde ckgo)
11. أرشيف (arshife)
12. يانوكس (yandex)

ثانيا // شركات التقنية العالمية ومنها: -

1. شركة أبل – مجال الأجهزة النقالة والحوسبة الشخصية والبرمجيات.
2. شركة سامسونج – الأجهزة النقالة ـ الإلكترونيات.
3. شركة موكسكون- تصنيع المكونات اللوحية.
4. شركة أمازون –التسوق عبر الانترنت.
5. شركة أتش بي – الحواسيب الشخصية –والطابعات المختلفة.
6. مايكروسوفت – والبرمجيات – معدات وأجهزة الحاسوب.
7. دبل تكنولوجيز- الحواسيب الشخصية.
8. هواوي – الاتصالات والمعدات والشبكات.
9. ال جي الكترونيكس –الالكترونيات.

ثالثا // شركات أنتاج البرمجيات ومنها: -

1. مايكروسوفت (الأول علي مستوي العالم)
2. أي بي أم.
3. جوجل
4. أكسنتر.
5. ساب.
6. شركة هوليت باكارد (HP).
7. -ياهو.
8. تقنيات (CA).
9. أوراكل.
10. كامجميني.

- **رابعاً // شركات الذكاء الصناعي.**
- **خامساً // شركات الحوسبة السحابية.**
- **سادساً // شركات قواعد البيانات ومنها على مستوي العالم: -**

1. المركز العالمي للبيانات المناخ.
2. مركز الحاسب الوطني الأبحاث الطاقة أو كلا ند في (كاليفوريا).
3. موقع شركة At8t .
4. موقع جوجل.
5. -شركة الهاتف سبرنت.
6. موقع تشولين بوسيت (خاصة بالشعب الأمريكي).
7. موقع يوتيوب.
8. - شركة أمازون.
9. وكالة الاستخبارات الأمريكية.
10. مكتبة الكونغرس الأمريكي.

ويمكن أيضا أن تكون قيمة تكنولوجيا المعلومات، ضمن القطاع الفردي لما له من دور فاعل في البناء والتنمية، ويمكنا أن نقسمه إلى قطاع فردي استشاري، وقطاع فردي لقواعد البيانات.

أولا // القطاع الفردي الاستشاري:

الفرد هو أساس مفهوم تكنولوجيا المعلومات، وأيضا هو المستهدف بتكنولوجيا المعلومات، فالشركات والمؤسسات المالية الاقتصادية تعتمد في مهامها على الاستعانة بالقطاع الفردي، ومثال الاستعانة بالمصممين أو المطورين أو المبرمجين بالتعاقد معهم لأداء مهمة عمل محددة، وهذا الأغلب، فالقطاع الفردي يقوم بدور استشاري عملي تنفيذي، ومن هنا تأتي أهميته وقيمته المالية.

ثانيا // القطاع الفردي لقواعد البيانات:

لقواعد البيانات أهمية اقتصادية كبري، وأعتمد القطاع الفردي على العلاقة الورقية لقواعد البيانات، باعتبار أن أصل قواعد البيانات هي مدخلات تتحول بعد المعالجة الآلية إلى معلومات، إذ بدون البيانات لا يمكن رصد المعلوماتية في تلك التكنولوجيا.

ثالثا // مجموعات العمل الفردية: -

هي مجموعة أفراد تحكمهم أفراد وثيقة شرف أو أتفاق، الهدف من ذلك هو حل مشكلة في أطار تكنولوجيا المعلومات، أو نتيجة وتطوير قطاع معين في سوق تكنولوجيا المعلومات، وتتخذ مجموعات العمل هذه في العادة شكلا لها عبر الانترنت، فهي ذات طابع فردي وما يحكم تعاملاتها هو عقد عمل جماعي أو فردي لصالح المجموع.

وفي ليبيا يمكننا إن نحدد أهم قواعد البيانات ومنها: -

1. مصلحة الأحوال المدنية ومنظومة الرقم الوطني.
2. المركز الوطني للمعلومات.
3. مصلحة الجوازات والجنسية.
4. إدارة تحقيق الشخصية.
5. وزارة العمل.
6. وزارة المواصلات.
7. وزارة التعليم (الامتحانات).
8. الضمان الاجتماعي (المتقاعدين).
9. منظومة الامن الداخلي.

أهم معايير الهاكر للهجوم على معلومات الشركات والمؤسسات:

أن معظم المحترفين **(الهاكر)**، لا يهاجمون دولاً فقيرة ولا دولاً ذات أهمية عالمية، وإنما يستهدفون دولاً بها زخم اقتصادي، وقطاعات حكومية وخاصة تحقق معدلات نمو مرتفع، ويستخدمون كل الوسائل الممكنة للعدوان وسرقة المعلومات بغرض التخريب والابتزاز والمساومة، ومن أهم الأهداف:

1. الأنظمة المصرفية والمالية.
2. نظم التشغيل وبرامج الشبكات والانترنت اللاسلكي **(الواي فاي)** وتطبيقات الويب.
3. الحوسبة السحابية.
4. شركات البرمجيات.
5. بيانات بطاقات الائتمان المصرفية.
6. منصات الإنترنت الأشياء باعتبارها مرتبطة بالإنترنت مباشرة.
7. قواعد البيانات والمواقع الالكترونية العسكرية.
8. الملكية الفكرية بجميع تقسيماتها المختلفة.

ويمارس المخترقين **(الهاكر)** الاختراق من أجل أظهار الإمكانيات وتحدي الذات، والبعض الآخر من أجل أهداف أخري مثل الحصول على الأموال أو المنافسة التجارية، أو بتحريض آخرين، والبعض من أجل المتعة والمرح، إلا أن المخترقين الذي يمتهنون العدوان علي المعلومات أهدافهم مالية، وقد تكون تنافسية، وفي

جانب أخر سياسية، وهناك العديد من الوقائع لاختراق شركات ومؤسسات كبري، مثل مايكروسوفت وشركة أرامكو، وسوني، وجوجل .....وغيرها

المبحث الثاني
نتائج الحماية الجنائية للمعلومات وموقف القانون المقارن.

تمهيد وتقسيم/
تعتمد قيمة المعلومات الاقتصادية على التخصص والنشاط والحاجة إلى هذه المعلومات من الطرف الثاني وعامل التوقيت، ولذلك برزت عدة نتائج على ذلك من أهمها الحماية الجنائية باعتبارها مصالح محمية وكيف عالج القانون المقارن هذا الموضوع.
كل ذلك جاء في **مطلبين الأول/** نتائج اعتبار قيمة المعلومات أصولاً مالية والمطلب الثاني الحماية الجنائية للمعلومات كقيمة اقتصادية عبر الانترنت في القانون المقارن

المطلب الأول
نتائج اعتبار قيمة المعلومات أصولا مالية

تطرقنا سابقاً إلي قيمة المعلومات الاقتصادية من خلال نوعية التخصص والنشاط، والحاجة إلى هذه المعلومات من الطرف الثاني، وهي بالتالي تحول هذه القيم العينية إلي قيم مالية نقدية، أو سندات لتدخل في حركة السوق وبالتالي العرض والطلب، وإذا اعترفنا بالرقمية وتكنولوجيا المعلومات كسند لإصدار أوراق مالية، فإنها يمكن أن يعتمد عليها في تنمية موارد اقتصاديات السوق، باعتبارها تفتح أفاقاً جديدة في أطار حركة التنمية الاقتصادية في الدولة، ومن رأينا أن هناك نتائج يمكن أن تترتب على اعتبار قيم تكنولوجيا المعلومات من الأصول المالية في السوق وأهمها :-

1- دخول حركة اقتصاد السوق مدخل جديد، يمكن به الكشف عن قيم تطور تتيح المجال أمامها، لفتح مجالات عمل كثيرة ومتنوعة تؤثر في تعديل حركة السوق الاقتصادية، وظهور مهن جديدة وقدرات أخري امتدت إلى السوق التجاري والاقتصادي والاستهلاكي والإنتاجي.

2- يعطي الاعتراف بأصول تكنولوجيا المعلومات كقيم مالية في أسواق المال، دفعة كبيرة لتفعيل العديد من التشريعات التي تساهم في حماية الحركة الإبداعية والابتكارية، ومثالها تشريعات حماية حقوق الملكية الفكرية، تفعيلا يناسب مع التطورات العالمية الحادثة في كل مجالات التقنية، حيث تساهم حركة السوق الاقتصادية في فرض العديد من أوجه الحماية بجانب السلطة التنفيذية والقضائية، فالسوق لا يعترف ألا بالأفضل والأدق وهو معيار وضابط الجودة، ولا يمكنه الاعتماد على قواعد جامدة أو قواعد المعاملات أو المجاملات.

3- تساهم الحركة الاقتصادية في دراسة النظام القانوني في الدولة، ومعرفة أوجه القصور من خلال المعاملات الاقتصادية اليومية، وما تبرزه من نتائج على الصعيد الاقتصادي والقانوني بشقيه الموضوعي والإجرائي، إذاً من مميزات الحركة الاقتصادية والتجارية والمالية، هو المرونة التي تتصف بها معاملاتها، وهي بلا شك تؤثر على القاعدة القانونية التي تتصف بالجمود، خاصةً وأن بعض الموضوعات لم تأخذ حظها الكامل من التطبيق القضائي في بعض الدول، مثل موضوعات الملكية الفكرية وقواعد البيانات

4- أن أصول تكنولوجيا المعلومات كقيم مالية في المؤسسات الاقتصادية، تصلح أن يتم إدماجها في قيمة الأسهم أو تسمية أسهم لها خاصة في مؤسسات الرقمية العربية، ويمكن اعتبارها مدخلاً مرحلياً في أطار سياسة البورصة العالمية، ورغم وجود صعوبات إلا أنه يمكن التغلب عليها بوجود القرار الاقتصادي الجيد.

5- يترتب اعتبار تكنولوجيا المعلومات قيمة مالية ودخولها السوق الاقتصادي العربي أو العالمي، التزام من مالكي هذه المعلومات بضرورة حمايتها تشريعياً وتقنياً، ومواكبة التطور في مجال التقني، بغض النظر عن مالكي هذه المعلومات (مؤسسات أو هيئات حكومية، أو على مستوي النشاط الفردي).

6- الالتزام الذي يقع علي مالكي هذه المعلومات، و اعتبارها قيم مالية في حق اختيار الأفراد العاملين عليها وتأهيلهم، و الاستعانة بالخبراء والاستشاريين، كلما أمكن ذلك وتحفيزهم للعمل وتطويره والمحافظة علي أمن هذه المعلومات من الاختراق أو المساومة، أو تجنيدهم من قبل مجموعات بغرض سرقة هذه المعلومات وبيعها، وهذا يحتاج إلي دراسات شخصية ونفسية للعاملين علي هذه المعلومات ومتابعتهم والأشراف عليهم بدقة، مع إعداد اختبارات وفرضيات للتأكد من عامل الثقة لديهم ، واتخاذ قرارات سريعة باستبعاد من تثبت عدم كفأته لهذه الوظيفة.

7- ضرورة توفير الحماية الجنائية للتكنولوجيا المعلومات، بوضع تشريعات خاصة بها، والعمل على تطويرها بشكل دائم، بما يتفق مع التطور السريع للتقنية وطرق ووسائل الاعتداء على هذه المعلومات، والاهم هو التطبيق الفعلي لهذه التشريعات.

8- ضمان وضع تكنولوجيا المعلومات واعتبارها قيم مالية، والنشاط الاقتصادي الناتج عنها من مشتملات ومحتوي القوانين الاقتصادية والاستثمارية للدولة، تلافيا للقصور التشريعي عند التنفيذ.
فهل هناك حماية جنائية للمعلومات؟ هذا سنتناوله في المطلب الثاني

المطلب الثاني
الحماية الجنائية للمعلومات كقيم اقتصادية عبر الانترنت في القانون المقارن

بالنظر إلي الأهمية البالغة التي تتميز بها المصلحة في النظام القانوني الوضعي، باعتبار أن القانون وجد من أجل البشر وحماية مصالحهم المختلفة، وأن غاية النصوص العقابية هي حماية المصالح، فالمشرع الجنائي عند صياغته للنصوص التشريعية يضع أمامه فائدة محددة تتمثل في حماية مصالح إنسانية مشروعة، إذ لا يخلو النص من المصلحة قدر المشرع أهميتها، فأسبغ حمايته عليها مهما كانت ضئيلة القيمة المادية أو المعنوية، وبالطبع المصالح كثيرة ومتقاربة، ولا يمكن تحقيق التوافق بينها إلا بوجود القانون الذي ينظم ويضع القواعد الأساسية سواءً في جانبه التقليدي أو الافتراضي .

الفرع الأول
مفهوم المصلحة وأهميتها

تُعَرَّف المصلحة لغة : بأنها ما يبعث علي الصلاح ، وما يتعاطاه الإنسان من الإعمال الباعثة علي نفعه أو نفع قومه وجمعها مصالح، وعرفها فقهاء القانون بأنها عنصر من عناصر الحق، بقولهم (الحق مصلحة مادية أو أدبية يحميها القانون)، والمشرع الجنائي لا يجرم الأفعال من أجل التجريم، بل يوظفها كوسيلة لحماية مصلحة بعينها، فكل جريمة تقليدية أو افتراضية تشكل اعتداء علي مصلحة معينة، أراد المشرّع أن يكفل لها الحماية والمصلحة، وتبدو أهمية المصلحة في أنها أساس التجريم في القانون، وهذا الأمر من شأنه أن يهدف إلي حماية المصالح، وتجريم السلوك الذي يخل بمظاهر الضبط في المجتمع والعدوان علي المصالح التي أسبغ عليها حمايته، كذلك المصلحة هي المعيار الذي يستعين به المشرع في وضع الضوابط الموضوعية للتقسيمات العامة للجرائم، ورسم النموذج القانوني لكل جريمة أو طائفة معينة من الجرائم، حيث أن للمصلحة أهمية بارزة في مرحلة التشريع ويستند المشرع علي المصلحة في الحماية التي يضيفها علي القواعد القانونية، ونلاحظ أن الأنظمة القانونية تختلف من حيث المصلحة التي تعمل علي إسباغ الحماية لها، وذلك تبعاً لقواعد القيم و المصالح والدين، فالمشرّع يختار المصلحة التي تهم المجتمع ويشملها بالحماية القانونية، فالمصلحة المحمية هي الأساس الذي يرتكز عليه المشرع في تجريم الجرائم المتجانسة ضمن نظام قانوني معين.

وتشكل المصلحة أهمية بمكان في تغيير أي نص قانوني، إذ أن المصلحة تقوم بدور بارز في هذا التفسير والوصول إلي حل المشكلات القانونية، والمصلحة هي مناط تشريع القانون الوصفي وتعديله وإلغائه، والمشرع في كل بلدٍ من بلاد العالم في التشريع والتعديل والإلغاء، يتصرف بمقتضي المصلحة العليا، حيث أنها تعد أساساً لتوحيد النصوص والتشريعات، وعلي سبيل المثال لا الحصر أن مشروع قانون الجرائم الافتراضية والدليل الرقمي المقدم من موسوعة التشريعات العربية في **ليبيا** تعرض لهذا الجانب في نص المادة **(14)** حيث نصت علي الآتي : **(المصلحة أساس الحكم، يراعي قاضي الموضوع في كل الأحوال، حجم المصلحة القائمة والمشروعة المعتدي عليها في كل جريمة وفي تقرير العقوبة وفق هذا القانون)**.

ونلاحظ أن هذا القانون في بنائه الكلي يستند إلى القاعدة العامة في القانون الجنائي الليبي، وهي فقه المصالح إذ أن المصلحة هي المبدأ العام، فالمقصود بالحماية وفق هذا النص هي تلك المصالح القائمة والمشروعة، فيجب النظر في المصلحة ذاتها وبحث صورتها واتصافها بالقيم المشروعة، فالنص لا يحمي المصالح

المحتملة وغير المشروعة، فيجب في كل الأحوال أن يتثبت قاضي الموضوع من قيام المصلحة فعلاً.
وكذلك مشروعيتها، وإقرار هذا النص يفيد في حقيقته أن على القاضي مراعاة المصلحة، ولو كان المشرع الجنائي قد أختص جزء من هذه المصلحة دون غيرها بالحماية، وما عداه لم يأت على ذكره جنائيا، ففي مثل هذه الحالة يجب أن يستمر قاضي الموضوع في تذكير حكمه بأهمية النواح الأخرى للمصلحة، ومدي تأثر الجزء المشمول بالحماية الجنائية بالأجزاء الأخرى التي لم يرد ذكرها جنائيا.

الفرع الثاني

موقف التشريعات المقارنة من الحماية الجنائية للمعلومات عبر الانترنت

تجد المعلومة ذاتها في القيمة المعنوية التي تحتويها، وهي بهذا المعني تحولت من مجرد المعرفة إلى التعامل بالمعرفة، وكان نتيجة لذلك التحول أن أصبح هناك ما يعرف بالمال المعلوماتي، الذي يصلح أن يكون محلا للحقوق وتحمل التبعية، فالمعلومة أصبحت تقوم ماليا وهي بالتالي تدخل في عداد الأموال الاقتصادية، كما تعرضنا لها سابقاً إلا أنه قد تكون المعلومات شخصية، وإفشائها يهدد الحياة الخاصة من جوانب متعددة ونتيجة للتطور التقني.

أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية لتوفر الحماية الجنائية لهذه المعلومات، وتطبيق هذه النصوص علي الجرائم المستحدثة، وباتت الحاجة ملحة لسن قواعد قانونية جديرة بمواجهة ما يحدث في العالم لافتراضي، ويجب أن تسند الحماية للمعلومات علي منطق التعامل التشريعي في إطار قانون الجرائم الافتراضية، كذلك الحماية الجنائية للمعلومات هي السبيل لتحقيق التجارة الدولية أهدافها وانجاز المعاملات، وإبرام التصرفات والصفقات التي تقتضيها فكرة التجارة الإلكترونية، ومن شأن كفالة حماية المعلومات علي الإنترنت أن يفضي سهولة المعاملات التجارية، وسرعة انجازها، إلي توفير الوقت والنفقات، وكانت المرحلة الأولى من التعديلات في السبعينات والثمانينات من القرن الماضي في العديد من الأنظمة القانونية العربية، وهذه التعديلات متعلقة بالحياة الخاصة، وهي رد فعل اتجاه التهديدات المستحدثة في الحياة الخاصة، كذلك فإن قوانين الاتصالات عالجت بعض الإشكاليات في حماية المعلومات .

أولاً / الحماية الجنائية للمعلومات على المستوى الدولي: -

اختلفت اتجاهات التشريعات المقارنة في النص على الحماية الجنائية للمعلومات فهناك اتجاه يرى إصدار تشريعات خاصة وعلى صورة معينة ومن أمثلتها الولايات المتحدة الأمريكية، والاتجاه الثاني يرى أن يتم إدخال تعديلات على النصوص القائمة بحيث يؤدي إلى استيعاب الجرائم المستخدمة. ومن أمثلة التشريعات التي تبنت هذا الاتجاه القانون الألماني والفرنسي.

1- تشريعات الولايات المتحدة الأمريكية:

أعتبر المشرع الأمريكي جرائم الحاسوب والجرائم الملحقة به من الجرائم الاتحادية، من خلال القانون سنة 1984م، تم تطورت بإصدار قانون إساءة استعمال الكمبيوتر 1994م، تم إصدار قانون اتحادي خلال سنة 2000 م ، للتوقيع الإلكتروني العالمي والتجارة الوطنية، ثم أصدرت عدة ولايات منها ولاية (**نورت كارولينا**)

قانون المعاملات الإلكترونية الموحد الذي دخل حيز التنفيذ سنة 2000م، كذلك أصدرت (**ولاية نيويورك**) خلال سنة 1998م للسجلات والتوقيع الإلكتروني، وأصدرت ولاية (**كونتكتكت**) قانون للمعاملات الإلكترونية في فبراير سنة 2002م، كذلك أصدرت ولاية بنسلفانيا قانوناً مماثلا سنة 1999م .

2- تشريعات فرنسا :

نص قانون العقوبات الفرنسي في الفصل الثالث الباب الثاني من خلال المادة (323-3)، إدخال أو مسح أو تغيير المعلومات بطرق الغش، كذلك جرم عدة أفعال تقع ضد المصالح العليا للدولة إذا انصبت على المعلومات أو البيانات التي تم معالجتها الكترونياً، في المواد (411- 6 إلى 411- 10) كذلك إصدار قانون الإثبات والتوقيع الإلكتروني سنة 2000م، ولائحته الصادرة سنة 2001م، كذلك قانون حرية الاتصالات التي صدر 1986م، تم عُدل بقانون سنة 2000م.

3- القانون الألماني :

صدر القانون سنة 1986م، والذي عدل بمقتضاه قانون العقوبات، وذلك بإضافة المادة (202أ) والتي جرم بها فعل التجسس على المعلومات المخزنة، كما أصدر المشرع الألماني قانون التوقيع الإلكتروني سنة 1997م، كذلك أصدر قانون المعلومات وخدمات الاتصالات الذي دخل حيز النفاذ سنة 1997م.

ثانياً / الحماية الجنائية للمعلومات في الدول العربية:

تماشياً مع ضرورة تطوير التشريعات تبعاً لمتغيرات المصالح المحمية التي وضعت لحمايتها، فقد سارت الدول العربية علي نهج إصدار التشريعات الكفيلة بمعالجة بعض الظواهر والجرائم المستحدثة، التي برزت نتيجة التطور التقني الذي صاحب الإنترنت مع عدم إغفال التشريعات التقليدية، والعمل علي تعديلها بما يتماشى مع التطور التقني في المفاهيم القانونية، و انتهجت الدول العربية اتجاهات مختلفة حسب النظم القانونية التي تتبعها، ولم تغفل أيضا أن توفر الحماية الجنائية للمعلومات كقيم اقتصادية حتى ضمن تشريعات الاتصالات، باعتبارها من القوانين الخاصة المعنية بنشر المعلومات والبيانات عبر الفضاء الافتراضي، وسنتعرض لبعض تشريعات الدول العربية وهي :

1- ليبيـــــا :/

أصدر المشرع الليبي العديد من التشريعات وأهمها:

أ- نصوص قانون العقوبات العام الليبي في المواد (171) إفشاء أسرار أمن الدولة والمادة (173) الحصول على أخبار سرية متعلقة بالدفاع والمادة (174) إذاعة أسرار الدفاع والمادة (182) استغلال أسرار الدولة والمادة (188) إذاعة أسرار التحقيقات والمادة (236) إفشاء أسرار الوظيفة والمادة (244) الاطلاع على المراسلات وإفشاؤها.

ب-نصوص القانون رقم 22 لسنة 210م بشأن الاتصالات من خلال المواد (15) سرية الاتصالات والمادة (16) حماية المعلومات الشخصية والمادة (26) إفشاء الأسرار والمادة (35) عقوبة إساءة استخدام شبكة المعلومات الدولية.

ج- نصوص القانون رقم 2 لسنة 2005م بشأن مكافحة غسل الأموال من خلال نص المادة (4) الالتزام بسرية المعلومات.

د- نصوص القانون رقم 2 لسنة 1979م بشأن الجرائم الاقتصادية من خلال نص المادة (12) إفشاء أسرار الشركات.

ه- نصوص القانون رقم 1 لسنة 1993م بشأن النقد والائتمان ونص المادة (72) سرية حسابات الزبائن ونص المادة (91) إفشاء البيانات والمعلومات.

و- نصوص مشروع قانون الجرائم الافتراضية والدليل الرقمي، خلال سنة (2005م) المقدم من موسوعة التشريعات العربية، (مقدم باسم المباحث الجنائية بوزارة الداخلية)، من خلال المواد (24) التداول غير المشروع للبيانات الاسمية، والمادة (25) الدخول لقواعد البيانات الاسمية والمادة (26) الاطلاع على البيانات السرية، والمادة (45) العدوان على الحق في الخصوصية والمادة (53) التلاعب بالمستندات ذات القيمة الاقتصادية والمادة (55) العدوان على المصنفات والمادة (56) العدوان على قواعد البيانات.

ز- نصوص مشروع قانون المعاملات الالكترونية المقدم من وزارة الاقتصاد خلال سنة 2015م من خلال المواد (39) المصادقة الالكترونية والمادة (45) سرية منظومة المصادقة والمادة (64) حماية المعاملات الالكترونية والمادة (81) حماية البيانات الخاصة والمادة (83) سرية البيانات الخاصة.

2- إمارة دبي :

نصوص القانون رقم 2 لسنة 2002م الخاص بالمعاملات والتجارة الالكترونية من خلال نص المادة (31) الاطلاع على المعلومات وإفشائها.

3- الكويت:

أ- نصوص القانون رقم (37) لسنة 2014م الخاص بالاتصالات ونص المادة (70) نشر المعلومات عبر وسائل الإعلام.

ب- نصوص القانون رقم (63) لسنة 2015م بشأن جرائم تقنية المعلومات ونص المادة (2) الدخول على البيانات الشخصية وفي المادة (3) الحصول على معلومات سرية حكومية.

4- سلطنة عمان:

نصوص القانون رقم (69) لسنة 2008م بشأن المعـــاملات الالكترونية من خلال نص المـادة (43 - 45) حماية البيانات الشخصية.

5- الإمارات العربية المتحدة:

أ- نصوص القانون الاتحادي رقم (40) لسنة 1992م. بشأن المصنفات الفكرية وحقوق المؤلف

ب- نصوص القانون الاتحادي رقم (5) لسنة 2012م. من خلال نصوص المواد (4 – 12) حماية المعلومات وهي من الجرائم الماسة بأمن الدولة والمادة (2) نشر معلومات أو بيانات والمادة (11) الوصول لأرقام البطاقات الائتمانية، المادة (21) الاعتداء على الخصوصية، الإمارات أول دولة عربية تصدر قانونا خاصا بمكافحة جرائم المعلومات.

6- الأردن:

نصوص القانون رقم (85) لسنة 2001م بشأن المعاملات الالكترونية المؤقت من خلال نص المادة (26) الإجراءات الكفيلة بالحفاظ على السرية المصرفية.

7- تونس :/

نصوص القانون رقم (83) لسنة 2000م بشأن المبادلات والتجارة الالكترونية من خلال مواد الباب السادس (الفصل 38 – 39 – 40) في حماية المعطيات الشخصية كذلك الفصل (9) المسئول عن معالجة المعطيات الشخصية.

8- البحرين:

أ- نصوص القانون رقم (28) لسنة 2002م بشأن المعاملات الالكترونية من خلال نص المادة (24 - 25) حماية بيانات التوقيع الالكتروني.

ب- نصوص القانون رقم (60) لسنة 2014م نص المادة (2) الجرائم الواقعة على بيانات وسيلة تقنية المعلومات.

9- السعودية:

نصوص نظامي مكافحة جرائم تقنية المعلومات والتعاملات الالكترونية 2007م, من خلال نص المادة (3) الماس بالحماية الخاصة والمادة (5) الدخول لقواعد البيانات والمادة (7) الدخول لموقع للحصول على معلومات تمس الأمن الوطني .

10- مصر:/

أ- نصوص القانون رقم (260) لسنة 1960م المادة (9) بشأن الأحوال المدنية المعدل بالقانون رقم (11) لسنة 1965م والقانون رقم (158) لسنة 1980م. على أن البيانات التي تحويها الأحوال المدينة تعتبر سرية، وكذلك المادة (2) عدم الكشف عن الحسابات المصرفية والمعلومات الموجودة بها.

ب- نصوص قانون الطفل رقم (12) لسنة 1996م في المادة (116) مكرر (ب) إذاعة المعلومات والبيانات عن طريق الإعلام المتعلقة بالطفل.

ج- نصوص القانون رقم (82) لسنة 2002م بشأن حماية حقوق الملكية الفكرية، نص المادة (55) المعلومات غير المفصح عنها، نص المادة (56) تؤيد حماية المعلومات، نص المادة (57) التزام الحائز القانوني للمعلومات.

11- الجزائر :

نصوص القانون رقم (9) لسنة 2009م المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثالثاً/ الجهود الدولية في حماية البيانات والمعلومات ذات الطبيعة الشخصية

يرجع أول قانون لحماية البيانات إلى مقاطعة هلسن في ألمانيا سنة 1970م، وأهم هذه الجهود الأتي:

1- المبادئ التوجيهية لمنظمة الاقتصاد والتنمية (**OECD**).
2- اتفاقية مجلس أوروبا (**Council of Europe**).
3- مبادئ الاتحاد الأوروبي التوجيهية بشأن معالجة البيانات الشخصية.
4- اتفاقية (**تيريس**) لحماية المعلومات السرية وحماية حقوق الملكية الفكرية.
5- الاتفاقية الأوروبية حول الجريمة الافتراضية - بودابست 2001م.
6- الاتفاقية الأوروبية بشأن حماية البيانات الشخصية بالنظر إلى المعالجة الآلية للبيانات.
7- قرار مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء (هافانا) 1990م المتعلق بالجرائم ذات الصلة بالكمبيوتر.
8- مشروع الاتفاقية الأمريكية لمكافحة جرائم الحاسب الآلي والإرهاب 1999م.
9- القانون الجزائي العربي الموحد لسنة 1979م.
10- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.
11- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2006م.

الخاتمة

يعد هذا البحث جهدا متواضعا لغرض عرض جوانب بسيطة من موضوع الضحية عبر الانترنت، وإن المعلومات يمكن أن تصبح ضحية بالمفهوم التقليدي، ولا ننكر الصعوبة التي واجهتنا في إعداد هذا البحث نتيجة قلة المراجع مع شكرنا **للدكتور الفاضل/ عمر بن يونس** لما قدمه من مراجع وأبحاث متعلقة بموضوع بحثنا، وفي الختام يمكن أن نحصر أهم النتائج فيما يلي:

1- لم يتم الاهتمام بعلم الضحية عبر الانترنت بالشكل المطلوب من الدارسين والباحث.
2- عدم كفاءة ومناسبة النصوص التقليدية مع جرائم العالم الافتراضي وعدم استيعاب النصوص التقليدية للنماذج الإجرامية المستخدمة نتيجة التطور التقني في العالم الافتراضي.
3- أن قيمة المعلومات تحدد بمدى الطلب الاستثماري عليها وعلاقتها بالأمن الوطني أو الاقتصادي أو الاجتماعي.
4- أن هناك مصادر للمعلومات وهي تشكل القيمة المالية لهذه المعلومات وأهمها الشركات الكبرى والمؤسسات المالية التي تحتفظ بقواعد البيانات لديها.
5- غياب النصوص الجنائية المتعلقة بحماية المعلومات على المستوى العربي رغم وجود تشريعات استرشادية ومبادئ وتوجيهات.
6- ضرورة الإسراع وبشكل جدي في إصدار التشريعات في ليبيا المتعلقة بالجرائم الافتراضية والدليل الرقمي.

التوصيات: -

1- تشجيع الباحثين والدارسين في علم الضحية لمواكبة الجرائم المستحدثة وما يحدث فيها من تطور.
2- اعتماد النتائج التي توصلنا إليها في بحثنا هذا.
3- استحداث نصوص جنائية خاصة متعلقة بالحماية الجنائية للمعلومات كقيم اقتصادية عند إصدار التشريعات الاقتصادية.
4- وجود التنسيق بين مؤسسات الدولة المختلفة في ليبيا لحماية المعلومات من الأخطار المحدقة بها.
5- ضرورة عقد اتفاقيات بين ليبيا ودول العالم فيما يتعلق بالمعلومات المتداولة عبر الانترنت وأهمية حمايتها جنائيا.
6- وضع خطة استراتيجية على مستوى ليبيا لحماية المعلومات وخاصة قواعد البيانات.
7- إصدار التشريعات المتعلقة بالخصوصية.
8- ضرورة إدراج المعلومات ضمن مسئوليات الأمن القومي الليبي وحمايتها واجبة قانوناً

المراجع

أولاً / الكتب القانونية: -

1- جو / لينكس - موسوعة ويكيبيديا الموسوعة الحرة - منشور على شبكة المعلومات الدولية , 2017م .
2- خلفاوي شمس طيات - بحث بعنوان مسألة قيمة المعلومات في اتخاذ القرار جامعة باجي مختار عناية - الجزائر - منشور على شبكة الانترنت.
3- رصاع نتيجة الحماية الجنائية للمعلومات على شبكة الانترنت - رسالة ماجستير 2012م - كلية الحقوق - جامعة أبي بكر بلقايد تلمسان - الجزائر.
4- د / زيد بن محمد الرياني، بحث الأثر الاقتصادي للجريمة الالكترونية - منشور على الانترنت 2013م.
5- د / عمر محمد بن يونس - أشهر مبادئ القضاء الأمريكي. (التجارة الالكترونية) - (الاستخدام الحر للإنترنت) غير منشورة.
6- عمر عبد الغفور أحمد القطان - المصلحة في تجريم القتل - مطبعة الانتصار - العراق 2010م.
7- د/ عمر محمد بن يونس، ورقة عمل بعنوان (الحصة الرقمية أصول تكنولوجيا المعلومات كقيم مالية) - مقدمة المؤتمر العربي الأول للاستثمار في شبكة المعلومات والمعرفة - الإسكندرية 2005م.
8- د. عبير علي حسين الورفلي - بحث بعنوان الجهود الدولية الإقليمية لمكافحة جرائم تقنية المعلومات - منشور كلية الاقتصاد والعلوم السياسية - العدد الخامس عشر سنة 2016م.
9- المرحوم، د / مصطفى ادبارة، وضع ضحايا الإجرام في النظام الجنائي - رسالة دكتوراه - القاهرة.

ثانيا / القوانين: -

1- القانون رقم 1 لسنة 1993م بشأن النقد والائتمان - ليبيا.
2- القانون رقم 83 لسنة 2000م بشأن المبادلات والتجارة الالكترونية - تونس - غير منشور.
3- مجموعة التشريعات الجنائية (العقوبات) إدارة القانون - ليبيا - 2001م.
4- الاتفاقية الأوروبية حول الجريمة الافتراضية - 2001م.
5- القانون رقم 85 لسنة 2001م بشأن المعاملات الالكترونية المؤقت - الأردن.
6- القانون رقم 28 لسنة 2002م بشأن المعاملات الالكترونية البحرين.
7- قانون رقم 2 لسنة 2002م بشأن المعاملات والتجارة الالكترونية - إمارة دبي - غير منشور.
8- مجموعة التشريعات الاقتصادية - الإدارة العامة للبحث الجنائي (غير منشورة)، قسم مكافحة الجرائم الاقتصادية - سنة 2003م.
9- القانون رقم 63 لسنة 2004م المتعلق بحماية المعطيات الشخصية بتونس - غير منشور.
10- قانون التجارة الالكترونية - مصر - 2004.
11- القانون رقم 2 لسنة 2005م بشأن مكافحة غسل الأموال الليبي.

12- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات - 2006م.
13- نظامي مكافحة جرائم المعلومات والمعاملات الالكترونية لسنة 2007م السعودية.
14- القانون رقم 69 لسنة 2008م بشأن المعاملات الالكترونية - سلطنة عمان - غير منشور.
15- القانون رقم 9 لسنة 2009م المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
16- القانون رقم 16 لسنة 2010م بشأن قانون المعاملات والتجارة الالكترونية - قطر القانون رقم 10 لسنة 2010م بشأن الاتصالات الليبي.
17- القانون 22 لسنة 2010م بشأن الاتصالات - ليبيا.
18- القانون رقم 5 لسنة 2012م (الإمارات العربية المتحدة) بشأن مكافحة جرائم تقنية المعلومات.
19- القانون رقم 2 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات - الإمارات العربية المتحدة.
20- القانون رقم 5 لسنة 2012م بشأن مكافحة جرائم تقنية المعلومات - الإمارات العربية المتحدة.
21- القانون رقم 37 لسنة 2014م بالاتصالات الكويتي.
22- القانون رقم 63 لسنة 2015م بشأن جرائم تقنية المعلومات - الكويت.
23- مشروع قانون المعاملات الالكترونية (وزارة الاقتصاد الليبية) (2015م) غير منشور.
24- القانون رقم 63 لسنة 2015م بشأن جرائم تقنية المعلومات الكويتي - غير منشور.
25- مقترح مشروع قانون الجرائم الافتراضية والدليل الرقمي يقدم من موسوعة التشريعات العربية - ليبيا.
26- المذكرة الإيضاحية لمشروع قانون الجرائم الافتراضية والدليل الرقمي، د / عمر محمد بن يونس.
27- مشروع الاستراتيجية العربية لمواجهة الجرائم الالكترونية.

ثالثاً / المواقع الالكترونية: -

- http/www.aljazeera.net
- www.5asapost.com

رسالة ماجستير

بعنوان:

التهديدات السيبرانية وتداعياتها على الأمن القومي
(دراسة حالة ليبيا 2011-2024)

إعداد:
الأستاذة / إسراء علي أبوعجيلة الأحول

باحثة دكتوراه في تخصص العلاقات الدولية
ومدربة دولية في الأمن السيبراني

التهديدات السيبرانية وتداعياتها على الأمن القومي

الملـخص

هدفت هذه الدراسة إلى تعريف وتحليل المفاهيم الأساسية المتعلقة بمفهوم التهديدات السيبرانية وتحليل أنواعها وأدواتها، والتعرف على الجهود الدولية المبذولة للتعامل مع هذه التهديدات، ومدى استفادة ليبيا منها، والتعرف على الأليات والسياسات والتشريعات التي يمكن تفعيلها من قبل صناع القرار في الدولة، لتحقيق الأمن السيبراني الليبي، وإرشاد الحكومة الليبية نحو تعزيز التعاون الإقليمي والدولي في مجال الأمن السيبراني، كما سعت إلى اقتراح إطار عمل شامل لاستراتيجية وطنية للأمن السيبراني في ليبيا، قادرة على مواجهة هذه التحديات المتصاعدة.

استندت الدراسة إلى منهجية بحثية متكاملة، باستخدام المنهج الوصفي التحليلي، ومنهج دراسة الحالة، وأيضا المنهج الاستقرائي، وشملت تحليلًا معمقًا للبيانات باستخدام أدوات جمع البيانات كالمقابلات، مع عينة الدراسة وهم المدراء في مجال الأمن السيبراني وأمن المعلومات والاتصالات في المؤسسات الحكومية والخاصة في ليبيا، ولتحليل البيانات التي جمعت تم استخدام تحليل MaxqudA، وقد خلصت الدراسة إلى مجموعة من النتائج أهمها، أن الأمن السيبراني ليس مجرد تحدٍ تقني، بل هو قضية تتطلب تعاونًا متعدد الأوجه بين الحكومات والقطاع الخاص والمجتمع المدني، و أنه على الرغم من الجهود المبذولة، لا يوجد إطار دولي شامل يعالج التهديدات السيبرانية، فالتحليلات تشير إلى أن التأثيرات الناتجة عن التهديدات السيبرانية تختلف بناءً على الهدف المحدد وقد كشفت النتائج غياب استراتيجية وطنية شاملة لمعالجة هذه المشكلة، علاوة على ذلك، توصلت النتائج إلى أن تحسين الأمن السيبراني يعد جزءًا أساسيًا من تعزيز الاستقرار الوطني والتنمية الاقتصادية والاجتماعية في ليبيا، بناءً على هذه النتائج، اقترحت الدراسة مجموعة من التوصيات أبرزها دعوة الحكومة الليبية إلى تنفيذ مقترح الاستراتيجية الوطنية للأمن السيبراني.

مـقدّمـــة

في عالم اليوم، باتت التقنية الرقمية تدخل جميع مناحي الحياة، بتحول الفضاء الإلكتروني إلى ساحة جديدة للصراع والتنافس، بين الدول والفاعلين في المجتمع الدولي، ونظرا لكونه مجالاً افتراضيًا، على عكس المجالات التقليدية المتعارف عليها (البرية، والبحرية، والجوية)، فقد جعل هذا التطور الخطير الصراعات والحروب لا تخوضها الدول بالدبابات والطائرات فحسب، بل امتدت إلى أبعاد جديدة، تمثلت في ظهور تهديدات سيبرانية معقدة تستهدف البنى التحتية الحيوية، والاقتصادات الوطنية، حتى الديمقراطيات وأنظمة الحكم، لم تتوقف عند كونها مجرد تحديات تقنية، بل تطورت لتشكل تهديداً وجودياً للأمن القومي للدول.

وفي ظل هذا الواقع، برزت تحديات جديدة تتعلق بتنامي حجم وتأثير التهديدات السيبرانية على الأمن والاستقرار الوطني، وهي تحديات لا تستثني ليبيا، التي شهدت منذ عام 2011م تعرض بنيتها التحتية الحيوية، ومؤسساتها الحكومية، وقطاعها الخاص، وأنظمة معلوماتها لهجمات رقمية متكررة. وقد أسهمت حالة الهشاشة الأمنية الناتجة عن التحولات السياسية والانقسامات الداخلية في جعل البلاد أكثر عرضة لهذه التهديدات، بما ترتب عليه خسائر اقتصادية كبيرة، وتعطيل للخدمات الأساسية، وتقويض لثقة المواطنين في المؤسسات الرسمية.

وانطلاقًا من هذه المعطيات، تتمحور إشكالية هذه الدراسة حول السؤال الرئيس :ما مدى تداعيات التهديدات السيبرانية على الأمن القومي للدول، وإلى أي مدى تمثل هذه التهديدات خطورة على ليبيا؟ وتهدف الدراسة إلى تحليل هذه الإشكالية في السياق الليبي خلال الفترة(2011-2024م)، من خلال رصد مظاهر التهديد، وقياس تأثيراته الأمنية والاقتصادية والاجتماعية، وتقديم رؤى عملية لمواجهته.

تنبع أهمية هذه الدراسة من دورها في الإسهام بتوجيه صانعي القرار نحو تبني توجهات واستراتيجيات جديدة تهدف إلى وضع سياسات وإجراءات وقائية فعّالة لحماية البنية التحتية الرقمية من التهديدات السيبرانية .كما تسعى إلى تعزيز المعرفة العلمية في هذا المجال، بما يوفر رؤى تحليلية وملاحظات قيّمة يمكن أن تشكّل إضافة نوعية للمكتبة الأكاديمية، يستفيد منها الباحثون والمهتمون وصانعو السياسات.

وتبرز أهمية هذه الدراسة كذلك في تركيزها على رفع مستوى الوعي بأهمية الأمن السيبراني، والمساهمة في بناء القدرات والخبرات على المستويين الأكاديمي والمهني، بما يمكّن من تطوير مهارات التحليل والبحث في قضايا الأمن السيبراني مستقبلًا .

كما تسلط الضوء على التحديات التي تواجه ليبيا في التعامل مع التهديدات الرقمية، وتطرح حلولًا عملية لتعزيز الأمن السيبراني وتحسين السياسات والإجراءات والمبادرات ذات الصلة .وإلى جانب ذلك، تسعى الدراسة إلى تعميق الفهم لمخاطر التهديدات السيبرانية، خاصة تلك القادرة على تعطيل البنى التحتية الحيوية والخدمات الحكومية، مع تحديد السبل المثلى للتصدي لها.

هدف هذه الدراسة إلى تحليل طبيعة التهديدات السيبرانية التي واجهتها ليبيا خلال الفترة الممتدة من 2011 إلى 2024م، وتقييم تداعياتها على مختلف أبعاد الأمن القومي الليبي .كما تسعى إلى تقديم توصيات عملية وواقعية لتعزيز الأمن السيبراني الوطني، ورصد الجهود المبذولة للتصدي للتهديدات الرقمية، سواء على المستوى الدولي أو المحلي . وإضافةً إلى ذلك، تهدف الدراسة إلى صياغة مقترح لاستراتيجية وطنية شاملة للأمن السيبراني، من شأنها الحفاظ على الأمن القومي والاستقرار الجيوسيبراني، مع تحديد الآليات والسياسات والتشريعات التي يمكن تفعيلها من قبل صانعي القرار، بما يسهم في تعزيز التعاون الإقليمي والدولي في هذا المجال.

اعتمدت الدراسة منهجية نوعية (كيفية)، استندت إلى جمع البيانات من مصادر متعددة، شملت التقارير الرسمية، والدوريات الأكاديمية، والكتب، وأوراق المؤتمرات، والوثائق الحكومية، بالإضافة إلى الإحصائيات، والرسوم البيانية، والدراسات السابقة. ولتنظيم المحتوى العلمي الموثق والمترجم، تم الاستعانة بأداة Schobot للذكاء الاصطناعي، بما يعكس دقة منهجية البحث في معالجة البيانات.

ونظرًا لطبيعة الموضوع، استخدمت الدراسة أدوات بحثية متنوعة، أبرزها المقابلات المفتوحة شبه المقننة، التي أُجريت مع مديري إدارات أمن المعلومات والاتصالات والأمن السيبراني في المؤسسات الحكومية والقطاع الخاص بليبيا. شملت عينة الدراسة خمسة وثلاثين مقابلة، موزعة على مجموعتين: الأولى تضمنت خمسة عشر سؤالًا موجهًا للمؤسسات الحكومية مثل الوزارات، والهيئات، والبنوك، وقطاع النفط، وشركات الاتصالات، والجهات السيادية؛ والثانية تضمنت ثمانية عشر سؤالًا موجهًا للشركات الخاصة. استغرقت عملية جمع البيانات الميدانية خمسة أشهر، من مايو إلى سبتمبر 2024م.

كما استعانت الدراسة بأدوات التحليل الاستراتيجي، مثل PESTLE وSWOT Analysis، بهدف تقييم الوضع الراهن للأمن السيبراني في ليبيا، واستخلاص التوجهات الاستراتيجية اللازمة لوضع مقترح وطني متكامل، يضمن تموضع ليبيا في موقع متقدم لمواجهة التهديدات السيبرانية والتقليل من آثارها.

تم تقسيم الدراسة إلى ثلاثة فصول ركز المبحث الأول منها على تعريف التهديدات السيبرانية وخصائصها الجوهرية، حيث عرّفت الباحثة التهديدات السيبرانية بأنها أي خطر أو هجوم أو فعل عدائي يقع في الفضاء الإلكتروني، ويستهدف الإضرار بالأجهزة والحواسيب والشبكات الإلكترونية، سواء كان منفَّذًا من قبل دول أو فواعل غير دولية، بهدف إلحاق الأذى أو إحداث الضرر بالبنية المعلوماتية والأنظمة المستهدفة، وقد تتنوع دوافع هذه التهديدات بين اقتصادية، أو سياسية، أو عسكرية، أو أيديولوجية، ويتم تنفيذها باستخدام أدوات وتقنيات رقمية متطورة، وقد تميزه هذه التهديدات بخصائص فريدة تميزها عن التهديدات التقليدية، أهمها **هي السرعة الفائقة في إحداث الضرر، صعوبة تحديد هوية المهاجمين، انتقائية الأهداف والتحكم في تداعيات الهجوم، التعقيد وعدم وضوح نقطة البداية أو النهاية، غياب الحدود الجغرافية**، حيث تتساوى الدول الصغيرة والكبيرة في الفضاء الإلكتروني.

ولا تقتصر مسببات التهديدات السيبرانية على الخلافات السياسية فحسب، بل قد تنشأ نتيجة التنافس الاقتصادي، أو بهدف سرقة المعلومات الاستراتيجية لفهم نوايا الخصوم، أو الاستحواذ على تصميمات الأسلحة والتقنيات العسكرية الحديثة، أو بدوافع أيديولوجية، ومن سماتها أيضًا أن المهاجم لا يحتاج إلى التواجد في نفس الموقع الجغرافي أو الميدان العملياتي للهدف، بل يمكن أن يشن الهجوم من قارة أخرى، مما يجعل هذه الهجمات غير مقيدة بالنطاق الإقليمي، ولا تخضع لقواعد ساحات المعارك التقليدية، إذ تُنفَّذ عبر الفضاء الإلكتروني للسيطرة على الأهداف أو تعطيلها دون الحاجة إلى تجاوز الدفاعات العسكرية التقليدية، كما تناول المبحث لمصادر المختلفة لهذه التهديدات، بما في ذلك الفاعلين الدوليين، والجماعات الإجرامية، والأفراد.

لاسيما تختلف أهداف التهديدات السيبرانية باختلاف طبيعة الجهات الفاعلة والمنافسين، إذ تُعد هذه الجهات من أبرز الأطراف المثيرة للجدل في النظام الدولي المعاصر، فقد تكون بعض الجهات الفاعلة من غير الدول أهدافًا محتملة للهجمات فقط، دون أن تكون هي المبادرة إليها، في حين تتبنى جهات أخرى أدوارًا هجومية تستهدف طيفًا واسعًا من الأهداف، لا يقتصر على الجانب العسكري فحسب، بل يمتد ليشمل مجالات ثقافية واقتصادية وسياسية واجتماعية.

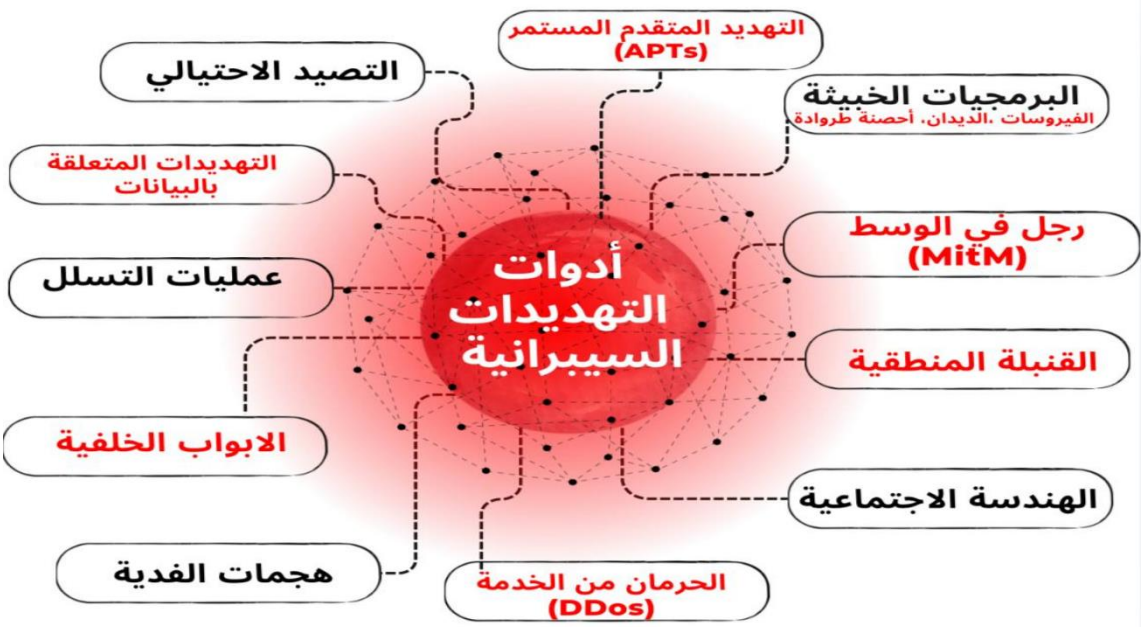
فعلى الصعيد الثقافي، قد تسعى الهجمات السيبرانية إلى طمس هوية الدولة وتشويه رموزها، بينما قد تتجه الأهداف الاقتصادية نحو تعطيل أو تدمير أنظمة المعلومات في المؤسسات المالية، خاصة مع تسارع عملية التحول الرقمي في معظم القطاعات. أما الأهداف السياسية، فقد تتجسد في استهداف المواقع الرسمية وأنظمة الشبكات الحكومية بقصد زعزعة الاستقرار أو التأثير على السياسات العامة، في حين تركز الأهداف العسكرية على مهاجمة الأنظمة القتالية والبنى التحتية الحيوية بغرض إضعاف القدرات الدفاعية. وفي ضوء ما تناولته هذه الدراسة، تم تحديد أبرز الأهداف التي تسعى التهديدات السيبرانية لتحقيقها، ومنها اختراق قواعد البيانات الحساسة، استهداف البنية التحتية الحيوية، مهاجمة الشبكات الحكومية والتجسس الصناعي، المساس بالهوية الوطنية والاجتماعية، إثارة الفتن والانقسامات السياسية الداخلية، تعطيل قطاعات التجارة والخدمات، استهداف الأنظمة العسكرية.

وفي ختام هذا المبحث، تمت مناقشة نظرية الردع السيبراني التي تُعنى بفهم التهديدات السيبرانية وآليات التعامل معها. تؤكد هذه النظرية أن مجرد امتلاك القدرة على الرد أو الانتقام، مقرونًا بالتواصل الفعّال، لا يعد كافيًا لتحقيق الردع، بل يجب أن يقتنع الطرف المهدِّد بجدية التهديد وإمكانية تنفيذه فعليًا. ويُعد هذا الشرط من أصعب التحديات على المستوى الوطني، خاصة وأن الدول غالبًا لا تُضحي بالكثير لمنع انتشار أدوات وتقنيات الهجمات الإلكترونية، على الرغم من إدراكها لحجم الأضرار المالية والأمنية التي قد تخلّفها.

ومع أن قادة العالم يبدون قلقًا متزايدًا إزاء التجسس السيبراني وتهديدات البنى التحتية الحيوية المتصلة بالإنترنت، فإن الردع السيبراني يظل إشكاليًا في ظل كوننا ما زلنا في مرحلة مبكرة من العصر الرقمي، حيث يصعب تقدير حجم الضرر المحتمل أو فعالية قدرات المهاجمين في حال الرد أو الانتقام. كما أن السرية التي تحيط بالقدرات الهجومية الحالية تزيد من تعقيد المشهد، وتترك الباب مفتوحًا أمام سيناريوهات مستقبلية قد تغيّر جذريًا من إدراك الدول لطبيعة التهديدات السيبرانية إذا ما أسفرت عن آثار كارثية واسعة النطاق.

أما في المبحث الثاني، فقد جرى تحليل أبرز الأدوات المستخدمة في تنفيذ التهديدات السيبرانية، مع دراسة كيفية توظيف هذه الأدوات من قبل المهاجمين لتحقيق أهدافهم المختلفة. كما تم تصنيف الأنماط المتنوعة لهذه التهديدات، بالاستناد إلى نهج متعدد التخصصات يجمع بين المنظورين التقني والفني، إضافةً إلى البعد السياسي، بهدف الوصول إلى فهم أعمق لطبيعتها وديناميكياتها.

ونظرًا للتنوع الكبير في هذه الأدوات وصعوبة حصرها أو تصنيفها بالكامل ضمن دراسة واحدة، ركزت الباحثة على أكثرها شيوعًا وتأثيرًا في استهداف الدول، كما هو موضح في الشكل رقم (3).



الشكل رقم (1) يوضح مصادر التهديد السيبراني، المصدر: إعداد الباحثة

وتناول هذا المبحث أنواع التهديدات السيبرانية وتم تصنّيَفها إلى عدة مستويات، وذلك بناءً على طبيعتها وتأثيرها في المستوى الأول نجد القرصنة الإلكترونية، أو التخريب الإلكتروني، وفي المستويين الثاني والثالث، تبرز الجريمة العابرة للحدود والتجسس السيبراني، أما في المستوى الرابع فيأتي الإرهاب السيبراني، وفي المستوى الأخير، الذي يعد الأخطر، نجد الحرب السيبرانية وتم تعريف كل نواع واذكر أمثله عليه. أما في المبحث الثالث فتناولنا مفهوم الأمن القومي من زوايا مختلفة، مع التركيز على العناصر الأساسية التي تشكله، كالأمن العسكري، السياسي، والاقتصادي، والاجتماعي، والتقني وتم مناقشة الإطار النظري لمدرسة كوبنهاغن لتحليل مفهوم الأمن القومي وتطوره.

حيث شهد مفهوم الأمن القومي تطورا كبيرا؛ إذ لم يعد يقتصر على الناحية العسكرية، ولم تعد وحدها صوراً التهديد ولا هي وحدها مصدره ويمكننا القول بأن، الأمن القومي بمفهومه المعاصر، هو مفهوم متعدد الجوانب والأبعاد وكذلك يمتاز باتساع نطاق المصالح السياسية والاقتصادية والعسكرية للدول وتشابكها وتعارضها، والتطور العلمي والتقني، في كافة المجالات الحيوية.

هدف هذا الفصل إلى تقديم إطار فهم شامل وعميق حول التهديدات السيبرانية، والأمن القومي كما يُمهد الطريق للدراسات المستقبلية التي تستكشف سبل التعامل مع التهديدات السيبرانية في سياق حماية الأمن القومي.

أما بالنسبة للفصل الثاني تناول عنوان التهديدات السيبرانية للأمن القومي: التداعيات وسبل المواجهة تناول هذا الفصل ثلاثة محاور رئيسية، تناول هذا المبحث أنواع التهديدات السيبرانية وتصنيفها إلى مستويات متعددة بناءً على طبيعتها وتأثيرها. ففي المستوى الأول تأتي القرصنة الإلكترونية والتخريب الإلكتروني، أما في المستويين الثاني والثالث فتبرز الجريمة السيبرانية العابرة للحدود والتجسس السيبراني. ويأتي في المستوى الرابع الإرهاب السيبراني، بينما يشكل المستوى الأخير — وهو الأخطر — الحرب السيبرانية. وقد تم تعريف كل نوع مع ذكر أمثلة توضيحية له، لتبيان مدى تنوع التهديدات وتفاوت شدتها وتأثيرها.

في المبحث الثالث، تم استعراض مفهوم الأمن القومي من زوايا متعددة، مع التركيز على العناصر الأساسية التي تشكله، مثل: الأمن العسكري، السياسي، الاقتصادي، الاجتماعي، والتقني. كما تم مناقشة الإطار النظري لمدرسة كوبنهاغن في تحليل مفهوم الأمن القومي وتطوره عبر الزمن.

يشهد مفهوم الأمن القومي تطورًا ملحوظًا، إذ لم يعد يقتصر على الجانب العسكري فقط، ولم تعد التهديدات العسكرية وحدها تشكل صور التهديد أو مصدره. إذ يمكن القول إن الأمن القومي بمفهومه المعاصر أصبح متعدد الأبعاد والجوانب، يمتاز باتساع نطاق المصالح السياسية والاقتصادية والعسكرية للدول، مع تعقيد وتشابك هذه المصالح أحيانًا، والتطور العلمي والتقني في مختلف المجالات الحيوية.

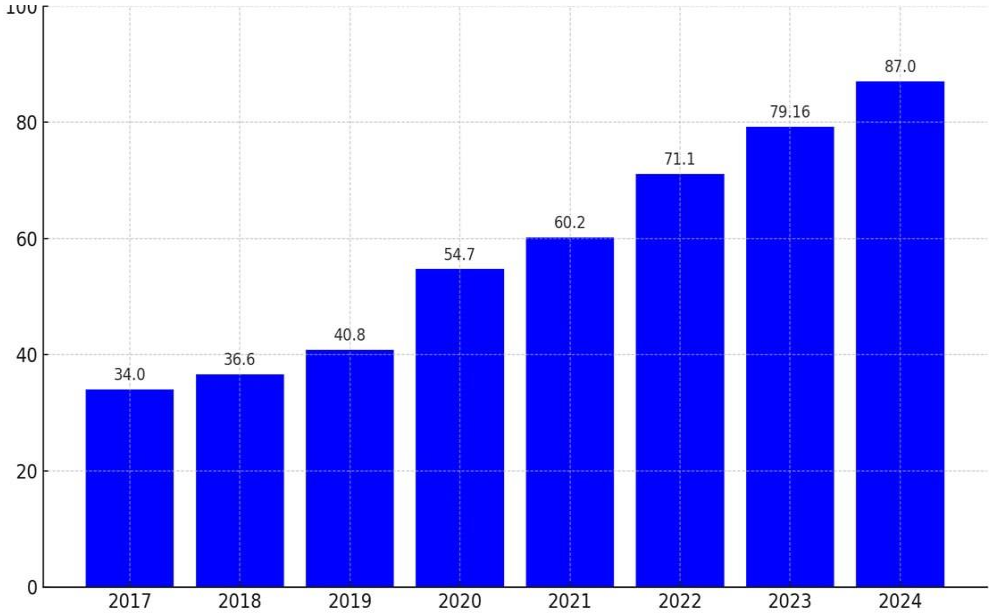
كان الهدف من هذا الفصل تقديم إطار شامل وعميق لفهم التهديدات السيبرانية والأمن القومي، ممهّدًا بذلك الطريق للدراسات المستقبلية التي تستهدف استكشاف سبل التعامل مع التهديدات السيبرانية في سياق حماية الأمن القومي.

أما الفصل الثاني الذي يحمل عنوان "التهديدات السيبرانية للأمن القومي: التداعيات وسبل المواجهة يعنى الفصل الثاني، المعنون بـ"التهديدات السيبرانية للأمن القومي: التداعيات وسبل المواجهة"، بثلاثة محاور رئيسية. ففي المبحث الأول، قدّمت الباحثة عرضًا مستفيضًا للتطور التاريخي للأمن السيبراني، بدءًا من نشأة الإنترنت في السبعينيات وصولًا إلى تطوره خلال القرن الحادي والعشرين. وعرفت الباحثة الأمن السيبراني باعتباره مجالًا علميًا متخصصًا في حماية الأنظمة والشبكات والبرمجيات من الهجمات الرقمية.

وقد عرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه مجموعة متكاملة من الأدوات والسياسات والمفاهيم الأمنية، إلى جانب الضمانات والمبادئ التوجيهية، ونُهج إدارة المخاطر، والإجراءات التدريبية، وأفضل الممارسات والتقنيات التي تُستخدم في حماية البيئة السيبرانية.

ومع مرور الزمن، شهد الأمن السيبراني تحولًا جذريًا من كونه مجالًا تقنيًا محدودًا إلى قطاع اقتصادي ضخم، يسجل معدلات نمو تفوق أربعة أضعاف متوسط نمو الاقتصاد العالمي، ليصل حجم سوقه السنوي إلى أكثر من تريليوني دولار في عام 2024 (المنتدى الدولي للأمن السيبراني، 2024). كما شهد الإنفاق العالمي على الأمن السيبراني زيادة ملحوظة خلال الفترة الممتدة من 2017 إلى 2024، كما يتضح من البيانات المعروضة في الشكل رقم (2).

الشكل رقم (2) الإنفاق على الأمن السيبراني في جميع أنحاء العالم، المصدر (statista:2024)



يوضح الرسم البياني نسبة الإنفاق العالمي على صناعة الأمن السيبراني، حيث بلغ الإنفاق 34 مليار دولار في عام 2017، واستمر في الارتفاع ليصل إلى 60.2 مليار دولار عام 2021، ثم شهد زيادة ملحوظة ليصل إلى 87 مليار دولار في عام 2024. وقد قامت الباحثة بتحليل الأبعاد المختلفة لهذا النمو المتسارع، مع التركيز على العلاقة الوثيقة بين الأمن السيبراني والأمن القومي.

وبذلك، أصبح الأمن السيبراني جزءًا لا يتجزأ من الأمن القومي، خاصةً في ظل تصاعد حجم التهديدات الإلكترونية وتداخل الأمن السيبراني مع عمل المنشآت الحيوية. ومع اعتماد الدول على شبكات الحاسوب كقاعدة أساسية لقوتها العسكرية والاقتصادية، فإن الأمن الوطني والاقتصادي يصبح معرضًا للخطر في حال ضعف الأمن السيبراني .

تشير الدراسات إلى أن الدول التي تولي اهتمامًا كبيرًا للأمن السيبراني تتمتع بقدرة أكبر على الحفاظ على قوات عسكرية قوية وقدرات اقتصادية متينة داخل النظام الدولي، وذلك بسبب حرصها على تأمين الفضاء الإلكتروني بنفس الدرجة التي تتعامل بها مع التهديدات التقليدية، إذ تدرك أن الخصوم المحتملين قد يستهدفون بنيتها التحتية الحيوية عبر الفضاء السيبراني.

وعليه، يرتبط الأمن السيبراني ارتباطًا وثيقًا بالأمن القومي. كما أن التطورات التقنية التي وسعت من دائرة الأفكار وأثرت على الثقافة، سمحت بامتداد الثقافة المحلية إلى المجال العالمي، لكنها في الوقت ذاته تطرح تهديدات للهوية الوطنية والقومية. ومع تأثر الأجيال الصاعدة بما يتلقونه من محتوى عبر الإنترنت، أصبحت الهوية الوطنية عرضة لعملية إعادة تشكيل مستمرة من خلال تأثيرات تكنولوجيا المعلومات.

أما في المبحث الثاني، قد استعرضت الباحثة دراسة لحالات ونماذج للتهديدات السيبرانية التي تعرضت لها دول مختلفة، مع بيان مدى تأثيرها على الأمن القومي، تم التركيز على حالات دراسية بارزة مثل التهديدات التي تعرضت لها إستونيا عام 2007، وأيضا التحديات السيبرانية التي واجهتها جورجيا خلال الحرب الروسية الجورجية عام 2008، بالإضافة إلى تلك التهديدات التي واجهتها السعودية عام 2012 وسيتم استعراض نماذج للتهديدات السيبرانية بين دول كبرى مثل روسيا وأوكرانيا، وبين الصين والولايات المتحدة الأمريكية، وبين إيران والولايات المتحدة الأمريكية ، وأيضًا الصراعات بين روسيا والولايات المتحدة الأمريكية.

إن الغرض من دراسة هذه النمادج والحالات هو زيادة مستوى المعرفة بأهمية الأمن السيبراني ومعرفة أخطر الحوادث للتهديدات السيبرانية في العالم التي غيرت افاق كل العالم السيبراني حيث تبرز هذه الحالات والنماذج التصاعد السريع للهجمات السيبرانية بين الدول، وتسلط الضوء على كيفية تأثيرها على السياسات الخارجية والقرارات الاستراتيجية للدول المتورطة كما توفر هذه النماذج فهمًا عميقًا لعملية تحليل التهديدات السيبرانية.

وفي المبحث الثالث تم توضيح الجهود الدولية المبذولة لمواجهة التهديدات السيبرانية، وبيان التعاون بين الدول والمنظمات الدولية، والإقليمية مثل الاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست) ، دليل تالين (Tallinn Manual) ، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، اتفاقية أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي (مالابو)، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، وأيضا ناقشت الدراسة المؤتمرات الدولية والإقليمية التي تلعب دوراً حيوياً في مكافحة التهديدات السيبرانية، من خلال توفير منصات لتبادل المعلومات وتحديد الاستراتيجيات، وتعزز هذه المؤتمرات التعاون الدولي والقدرات الوطنية في مواجهة التحديات السيبرانية المتنامية، لاسيما أنه عدد المؤتمرات الدولية والإقليمية التي تناولت موضوع الأمن السيبراني لا يمكن حصره ومع ذلك، سأسلط الضوء على بعض من أبرز هذه المؤتمرات التي لعبت دوراً بارزاً في تعزيز التعاون الدولي وتحسين الوعي بأهمية الأمن السيبراني، وايضا ناقشت جهود المنظمات والشركات الإقليمية والدولية على مستوى العالم وذلك من خلال مجموعة واسعة من الأنشطة والجهود المشتركة التي تتمثل في وضع الإطارات القانونية والمعايير التقنية وتسهيل التعاون الدولي، وتم تناول على سبيل المثال لا الحصر مجموعة من المنظمات والشركات الدولية مع التركيز على الجهود الأكثر اهمية والتي تعتبر مهمة في تعزيز الامن السيبراني وهي الأمم المتحدة، جامعة الدول العربية، منظمة حلف شمال الاطلسي(الناتو)، الاتحاد الأوروبي، شركة ميكروسوفت، منظمة الدول الأمريكية، **وتم** مناقشة المبادرات المشتركة، والمعايير الدولية، وأهمية تبادل المعلومات والخبرات في بناء استراتيجيات فعالة لمكافحة هذه التهديدات وقد تم اختيار استراتيجيات خمس دول وهي الدول الاولى دوليًا وإقليمًا وعربياً ورياديا حسب مؤشر الاتحاد الدولي للاتصالات عام 2024م مثل الاستراتيجية الوطنية لأمن المعلومات للمملكة العربية السعودية ، استراتيجية الأمن السيبراني لإستونيا ، استراتيجية الأمن السيبراني للولايات المتحدة الامريكية، الاستراتيجية الوطنية للأمن السيبراني للمملكة المتحدة، .استراتيجية موريشيوس للأمن السيبراني، وبهاذ يمكننا القول بأن استراتيجيات الأمن السيبراني للدول المذكورة أعلاه تتباين فيما بينها، إلا أنها تتفق في جوهرها على أهمية بناء قدرات وطنية قوية، وتبني شراكات دولية، والاستثمار في التكنولوجيا الحديثة ودعم البحث والتطوير والتعاون بين القطاع العام والخاص وتعزيز البنية التحتية وتبني تشريعات حديثة لحماية البيانات والخصوصية، يمكن لليبيا الاستفادة من هذه التجارب من خلال تكييفها مع سياقها المحلي، مع التركيز على بناء نظام بيئي رقمي آمن ومرن من خلال تبني نهج شامل ومتكامل للأمن السيبراني، يمكن لليبيا حماية بنيتها التحتية الحيوية، وتعزيز مكانتها في الاقتصاد الرقمي العالمي.

أما الفصل الثالث تناول تداعيات التهديدات السيبرانية للأمن القومي الليبي وطرق التصدي في هذا المبحث،

استعرضت الباحثة مجموعة من الحالات والنماذج البارزة للتهديدات السيبرانية التي تعرضت لها دول مختلفة، مع التركيز على تأثيرها المباشر على الأمن القومي. شملت الدراسة تحليلًا لحالات دراسية مهمة مثل الهجمات السيبرانية التي استهدفت إستونيا عام 2007، والتحديات السيبرانية التي واجهتها جورجيا خلال الحرب الروسية-الجورجية عام 2008، بالإضافة إلى الهجمات التي تعرضت لها المملكة العربية السعودية عام 2012.

كما تناولت الباحثة نماذج للتهديدات السيبرانية بين دول كبرى، مثل النزاعات الرقمية بين روسيا وأوكرانيا، والصراعات بين الصين والولايات المتحدة الأمريكية، وكذلك بين إيران والولايات المتحدة، إضافة إلى التوترات السيبرانية بين روسيا والولايات المتحدة الأمريكية.

وتهدف دراسة هذه الحالات إلى رفع مستوى الوعي بأهمية الأمن السيبراني، وتسليط الضوء على أخطر الحوادث السيبرانية التي أثرت على المشهد العالمي، حيث تعكس هذه النماذج تصاعد وتيرة الهجمات السيبرانية بين الدول، وتوضح كيفية تأثيرها على السياسات الخارجية والقرارات الاستراتيجية للدول المعنية. كما توفر هذه الحالات فهمًا معمقًا لعمليات تحليل التهديدات السيبرانية وآليات التعامل معها.

أما المبحث الثالث فتناول الجهود الدولية لمواجهة التهديدات السيبرانية في هذا المبحث، تم توضيح المبادرات والجهود الدولية الرامية إلى مكافحة التهديدات السيبرانية، مع التركيز على التعاون بين الدول والمنظمات الدولية والإقليمية. وقد استعرضت الباحثة أهم الاتفاقيات الدولية مثل اتفاقية بودابست بشأن الجريمة الإلكترونية، ودليل تالين (Tallinn Manual)، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بالإضافة إلى اتفاقية مالابو المتعلقة بأمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.

كما ناقشت الدراسة الدور الحيوي للمؤتمرات الدولية والإقليمية التي تساهم في تعزيز مكافحة التهديدات السيبرانية من خلال توفير منصات لتبادل المعلومات ووضع الاستراتيجيات، وتعزيز التعاون الدولي والقدرات الوطنية لمواجهة التحديات المتزايدة في هذا المجال. وعلى الرغم من تعدد هذه المؤتمرات وصعوبة حصرها، تم تسليط الضوء على أبرزها ودورها في رفع الوعي وتطوير التعاون الدولي.

بالإضافة إلى ذلك، استعرضت الباحثة جهود المنظمات والشركات الإقليمية والدولية مثل الأمم المتحدة، وجامعة الدول العربية، ومنظمة حلف شمال الأطلسي (الناتو)، والاتحاد الأوروبي، وشركة مايكروسوفت، ومنظمة الدول الأمريكية، مع التركيز على المبادرات المشتركة، والمعايير الدولية، وأهمية تبادل المعلومات والخبرات لبناء استراتيجيات فعالة لمكافحة التهديدات السيبرانية.

كما تم تحليل استراتيجيات الأمن السيبراني لخمس دول بارزة على المستوى الدولي والإقليمي والعربي، والتي تم اختيارها بناءً على مؤشر الاتحاد الدولي للاتصالات لعام 2024، وهي: المملكة العربية السعودية، إستونيا، الولايات المتحدة الأمريكية، المملكة المتحدة، وموريشيوس. وتُظهر هذه الاستراتيجيات تفاوتًا في التفاصيل، لكنها تتفق جميعًا على أهمية بناء قدرات وطنية قوية، وتبني شراكات دولية، والاستثمار في التكنولوجيا الحديثة، ودعم البحث والتطوير، وتعزيز التعاون بين القطاعين العام والخاص، فضلاً عن تطوير البنية التحتية وتحديث التشريعات الخاصة بحماية البيانات والخصوصية.

يمكن لليبيا الاستفادة من هذه التجارب من خلال تكييفها بما يتناسب مع خصوصياتها المحلية، مع التركيز على بناء نظام بيئي رقمي آمن ومرن، واتباع نهج شامل ومتكامل للأمن السيبراني، مما يتيح حماية بنيتها التحتية الحيوية وتعزيز مكانتها في الاقتصاد الرقمي العالمي.

اما الفصل الثالث تناول تداعيات التهديدات السيبرانية على الأمن القومي الليبي وسبل التصدي، ضم هذا الفصل ثلاثة مباحث رئيسية، بدأ المبحث الأول بتحليل وتحديد التهديدات السيبرانية التي تواجه ليبيا. تم إجراء دراسة متعمقة لأنماط الهجمات المستخدمة والجهات الفاعلة وراءها، بهدف بناء فهم دقيق للسياق السيبراني الذي تنشأ فيه هذه التهديدات.

تعتبر ليبيا دولة ذات أهمية استراتيجية خاصةً في ظل التغيرات السياسية والاجتماعية التي شهدتها منذ عام 2011. مع تطور استخدام الإنترنت في البلاد، ظهرت تهديدات سيبرانية تستهدف مؤسسات الدولة والمواطنين على حد سواء. وتجدر الإشارة إلى أن هذه الدراسة لا تهدف إلى حصر كل التهديدات السيبرانية التي تواجه ليبيا، وذلك لأسباب متعددة وهي نقص إحصائيات حكومية موثوقة ومعلنة حول حجم التهديدات، مما يحد من إمكانية الحصول على صورة شاملة ودقيقة، اعتماد البيانات المتاحة بشكل رئيسي على مقابلات مع خبراء في الأمن السيبراني، بالإضافة إلى

إحصائيات ومراجع من شركات عالمية ودراسات منشورة، لكنها تظل محدودة نوعًا ما، وأظهرت النتائج أن القطاعات الأكثر عرضة للهجمات السيبرانية في ليبيا تشمل قطاع الاتصالات، بسبب إمكانية استغلاله لتعطيل عمليات واسعة النطاق، وقطاع النفط والغاز الذي يُعد هدفًا ذا تأثير بالغ على الاقتصاد الوطني. كما تعرضت الخدمات المالية، بما في ذلك المصارف، لهجمات كشفت هشاشة البنية الأمنية في هذا القطاع. إضافة إلى ذلك، تواجه البنى التحتية الحيوية الأخرى مثل الكهرباء والمياه والمؤسسات الحكومية تهديدات سيبرانية مستمرة. وتعتمد هذه القطاعات بدرجة كبيرة على التقنية الرقمية والبيانات الحساسة، ما يجعلها أهدافًا سهلة تؤدي استهدافها إلى تأثيرات كبيرة على الصعيدين الاقتصادي والسياسي.

في المبحث الثاني، تم تسليط الضوء على جهود الجهات الليبية في مراجعة وتقييم التهديدات السيبرانية، مع استعراض التدابير والإجراءات المتخذة في هذا المجال. ومن أبرز هذه الجهود:

- نشاط الهيئة الوطنية لأمن وسلامة المعلومات (NISSA) في تطوير الإطار القانوني لحماية الفضاء الإلكتروني.
- إصدار مجلس النواب القرار رقم 5 لسنة 2022م الخاص بمكافحة الجرائم الإلكترونية، والذي يضم 52 مادة قانونية مهمة.
- صدور القانون رقم 6 لسنة 2022، والقرار رقم 150 لسنة 2024 الصادر عن وزارة الاقتصاد والتجارة، والقرار رقم 37 لسنة 2024 الصادر عن الهيئة العامة لأمن وسلامة المعلومات بشأن ضوابط استخدام حسابات الجهات الحكومية على منصات التواصل الاجتماعي.
- تعزيز التعاون الإقليمي والدولي في مجال الأمن السيبراني لتبادل الخبرات وبناء القدرات.
- نظيم المؤتمرات المحلية والدولية التي تهدف إلى تبادل المعرفة وتعزيز التعاون بين المؤسسات الحكومية والشركات الخاصة.

استنادًا إلى هذه الجهود المتواصلة، يمكن القول إن ليبيا أحرزت تقدمًا ملحوظًا في مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات (ITU)، حيث تعكس التحسينات المستمرة في المؤشر التزام الحكومة الليبية بتعزيز البنية التحتية الرقمية، وتطوير السياسات اللازمة لحماية المعلومات والبيانات الحساسة.

أما المبحث الثالث، فيدور حول مقترح لتطوير استراتيجية وطنية للأمن السيبراني في ليبيا

تناول المبحث الاول على تقديم مقترح لإنشاء إطار متكامل لبناء استراتيجية وطنية شاملة للأمن السيبراني في ليبيا .تهدف الدراسة إلى تأسيس منظومة وطنية متماسكة للأمن السيبراني، تتوافق مع أبرز الممارسات الدولية المتقدمة في هذا المجال.

يهدف المقترح إلى تبني منهج شامل يمكّن جميع الجهات الحكومية والخاصة من رفع مستوى أمنها السيبراني، وحماية شبكاتها وأنظمتها وبياناتها الإلكترونية .كما يسعى إلى تطوير مبادئ الأمن السيبراني وتعزيز وعي المؤسسات والأفراد بمسؤولياتهم الوطنية تجاه حماية الفضاء السيبراني.

علاوة على ذلك، يهدف الإطار المقترح إلى تحقيق مستوى عالٍ من النضج والمهنية في ممارسات الأمن السيبراني، مع توضيح مسؤوليات كل جهة تجاه حماية أمنها الإلكتروني .ويسهم هذا الإطار أيضًا في حماية الأمن القومي الليبي من خلال تأسيس قدرات دفاعية فعالة، تعيق أنشطة الجهات الفاعلة الخبيثة، وتدعم الاستثمار في منظومة رقمية أكثر أمانًا وموثوقية.

وقد تم إعداد هذا المقترح بالاعتماد على مراجعة شاملة للمراجع العلمية، والخطوات الأساسية لتطوير استراتيجيات الأمن السيبراني الوطنية، بما يضمن ملاءمته للسياق الوطني الليبي ومتطلبات الأمن القومي.

1. الرجوع إلى تجارب الدول الرائدة حسب مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات سنة 2024، الذي يقيس التزام الدول بالأمن السيبراني، تم اختيار الدول الأهم على المستويات الإقليمية والدولية والعربية والريادية، حيث تمت دراسة تجارب الولايات المتحدة والمملكة المتحدة، والمملكة العربية السعودية، وإستونيا وموريشيوس.
2. دليل صنع السياسات (2020) الذي يركز على إشراك أصحاب المصلحة في استراتيجيات الأمن السيبراني الوطنية، الصادر عن الشركاء العالميون الرقميون.
3. دليل تطوير استراتيجية وطنية للأمن السيبراني الصادر عن شركة مايكروسوفت (Microsoft) في عام 2013.
4. المبادئ التوجيهية لاستراتيجية الأمن السيبراني الوطنية، منظمة حلف شمال الاطلسي (الناتو) الصادر عن مركز التميز الفاعي السيبراني التعاوني التباع لحلف شال الاطلسي، 2013.

5. دليل استراتيجيات الأمن السيبراني الوطنية الصادر عن منظمة الدول الأمريكية (2022)
6. دليل الممارسات الجيدة لتطوير استراتيجية الأمن السيبراني الوطنية الصادر عن مجلس الاتحاد الأوروبي لوكالة الشبكات والمعلومات (ENISA) في نوفمبر 2016.
7. الاستراتيجية العربية للأمن السيبراني (2023-2027) الصادرة عن جامعة الدول العربية والمنظمة العربية لتكنولوجيا الاتصالات والمعلومات في 24 يناير 2024.

8. دليل إعداد الاستراتيجيات الوطنية للأمن السيبراني، بمشاركة أكثر من أثني عشر شريكًا في الإصدارين الأول والثاني، وشملت هذه المشاركة المنظمات الحكومية، والدولية، والخاصة، بالإضافة إلى الأكاديميين والجمعيات المدنية التي تمثل بعض الجهات البارزة في هذا الجهد الاتحاد الدولي للاتصالات، والبنك الدولي، وأمانة الكومنولث، ومركز التميز التعاوني للدفاع السيبراني التابع لحلف شمال الأطلسي، بالإضافة إلى جهات أخرى، تم تنفيذ هذا العمل خلال فترتين عام 2018 وعام 2021.

9. الاستراتيجية الصادرة عن الهيئة العامة لأمن وسلامة المعلومات الصادرة سنة 2023. وأيضا تم الاستعانة ببعض الوثائق الوطنية.
10. من خلال توظيف أدوات تحليلية متقدمة مثل SWOT وPESTEL، بالإضافة إلى استخدام أسلوب المقابلات الشخصية مع الكوادر القيادية في مجالي إدارة أمن المعلومات والأمن السيبراني في المؤسسات العامة والخاصة في ليبيا، وبدراسة أبرز الهجمات والتهديدات والمخاطر السيبرانية العالمية والإقليمية والمحلية ومدى تأثيرها.

إن دعم تنفيذ هذه الاستراتيجية على أرض الواقع وتمويلها من السلطة التنفيذية سيكون عاملًا معززًا لجهود ليبيا في المحافظة على منظومة الأمن والأمان وتعزيزها، بالإضافة إلى رفع مستوى الأمن السيبراني. يهدف مقترح الاستراتيجية إلى أن يكون إطارًا وطنيًا لدعم الجهود الحكومية وتطوير البنية التحتية التي تضمن النهوض بدولتنا على مدى خمس سنوات (2025-2029) وتشمل أهدافاً محددة وخطة عمل مفصلة ومؤشرات أداء لقياس التقدم، يستند مقترح الاستراتيجية إلى أفضل الممارسات لتعزيز أمن الفضاء السيبراني لليبيا وأيضاً إلى تحويل ليبيا إلى واحدة من الدول الرائدة في الأمن السيبراني خلال السنوات القادمة، بطموح شعبها وقادتها.

الأمن السيبراني لم يعد مجرد مسألة تقنية تتعلق بحماية الأنظمة والشبكات، بل أصبح مكونًا جوهريًا، ضمن استراتيجيات الحفاظ على الأمن القومي للدول. وقد كشفت التطورات التي حدثت في ليبيا، منذ سنة 2011م، عن تزايد التهديدات السيبرانية من حيث العدد والتعقيد، ما شكل خطرًا كبيرًا على استقرار القطاعات الحيوية،

بما في ذلك المؤسسات الحكومية، القطاع المصرفي، البنية التحتية للطاقة، وقطاع الاتصالات. سلطت هذه التهديدات الضوء على ضعف البنية التحتية الرقمية في ليبيا، نتيجة لتقادم الأنظمة وغياب تقنيات الحماية المتطورة، بالإضافة إلى نقص التشريعات المحلية التي تنظم وتحمي الفضاء السيبراني.

تشير نتائج الدراسة إلى أنّ أدوات التهديدات السيبرانية تتسم بالشمولية ولا تقتصر على البرمجيات الخبيثة، والاختراقات الإلكترونية، والتصيد الاحتيالي، والهجمات بالحرمان من الخدمة، بل تشمل طيفًا واسعًا من الوسائل والأساليب التي تتطور باستمرار. وعلى الرغم من تعدد الجهود المبذولة لمواجهتها، إلا أنّه لا يزال يفتقر المجتمع الدولي إلى وجود إطار قانوني وتنظيمي شامل يحكم هذه التهديدات، الأمر الذي يؤكد الحاجة الماسّة إلى تعزيز التعاون الدولي وتبادل المعلومات والخبرات بهدف مكافحة التهديدات السيبرانية بفاعلية أكبر وتحقيق مستويات أعلى من الأمن الرقمي.

وفي ضوء ذلك، أصبح الأمن السيبراني ضرورة لا غنى عنها في العصر الحديث، إذ يشمل منظومة متكاملة من السياسات والتقنيات والإجراءات الرامية إلى حماية الأنظمة الرقمية والمعلومات من الهجمات الإلكترونية، ويتطلب التزامًا كاملًا من كل دولة لضمان صمود بنيتها التحتية أمام هذه المخاطر.

وبالنسبة لليبيا، تُظهر النتائج أن جهود الحكومة في مجال الأمن السيبراني ما زالت محدودة، مما يستدعي تعزيز القدرات الوطنية وتطوير استراتيجيات فعّالة للتعامل مع هذه التهديدات. فالتهديدات السيبرانية ذات طبيعة مزدوجة، تقنية وسياسية، الأمر الذي يحتم تفعيل آليات تبادل المعلومات على المستوى الدولي، وإدراج هذا التعاون كعنصر أساسي ضمن الاستراتيجية الوطنية للأمن السيبراني. كما يتطلب الوضع الراهن الاستثمار في تطوير البنية التحتية السيبرانية، بما في ذلك إنشاء مراكز وطنية متخصصة لمراقبة وتحليل التهديدات، ووضع آليات استجابة سريعة وفعّالة، تتضمن خطط طوارئ وتدريبات دورية للتعامل مع الحوادث السيبرانية.

وتؤكد الدراسة كذلك على أهمية مراجعة وتحديث السياسات والإجراءات الوطنية المتعلقة بالأمن السيبراني بشكل دوري لمواكبة التطورات التقنية وأساليب الهجمات الجديدة. وقد أدت الهجمات الإلكترونية المتزايدة إلى إعادة تقييم استراتيجيات الأمن القومي، حيث أدركت الدول الكبرى أن هذه التهديدات قادرة على استهداف البنية التحتية الحيوية والتأثير على الأمن الداخلي. كما ألحقت هذه الهجمات خسائر اقتصادية جسيمة بالدول والشركات، شملت تعطيل الأنظمة وسرقة البيانات وفرض عمليات فدية.

وقد دفع هذا الواقع العديد من الدول الكبرى إلى تعزيز التعاون الدولي لمواجهة المخاطر السيبرانية، مما أسفر عن إنشاء تحالفات جديدة ووضع معايير مشتركة للأمن السيبراني. وفي هذا السياق، توصي الدراسة بضرورة تطوير استراتيجية وطنية شاملة للأمن السيبراني في ليبيا، تتضمن تعزيز البنية التحتية، وتحديث التشريعات، وإنشاء مركز وطني للأمن السيبراني، وتحسين مستوى الوعي المجتمعي، وتوفير التدريب المتخصص. كما تشدد على أهمية التعاون الإقليمي والدولي لتبادل المعلومات والخبرات، بما يعزز من قدرة الدولة على التصدي للهجمات السيبرانية.

وفي الختام، تؤكد الورقة أنّ الأمن السيبراني بات يشكل ركيزة أساسية من ركائز الأمن القومي، وأنّ مواجهة التهديدات الرقمية المتزايدة تتطلب اتخاذ خطوات فورية لتعزيز القدرات الوطنية وحماية مصالح الدولة في الفضاء الإلكتروني.

أهم المراجع:

1. الاتحاد الإفريقي، اتفاقية الاتحاد الإفريقي)مالابو (بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، متاح عبر https://2u.pw/2A67PB :
2. الاتحاد الدولي للاتصالات وآخرون، دليل لوضع استراتيجية وطنية للأمن السيبراني)التزام استراتيجي بالأمن السيبراني(، 2018، متاح عبر http://creativecommons.org :
3. المنتدى العالمي للأمن السيبراني (2020)، نظرة عامة على أدوات تقييم القدرات السيبرانية القائمة على الصعيد الوطني (GOAT)
4. الاتحاد الدولي للاتصالات وآخرون، العمل الاستراتيجي في مجال الأمن السيبراني، دليل إعداد الاستراتيجيات الوطنية للأمن السيبراني، الطبعة الثانية، 2021، https://creativecommons.org/licenses/by-.nc/3.0/igo/U
5. الاستراتيجية الوطنية للأمن السيبراني، الهيئة الوطنية الليبية للأمن وسلامة المعلومات على شبكة الإنترنت : https://2u.pw/9UJMVF
6. الأمم المتحدة، الجمعية العامة، اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، 2024
7. جامعة الدول العربية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، 2010، www.arablegalent.org
8. جامعة الدول العربية والمنظمة العربية للتكنولوجيات الاتصال والمعلومات، الرؤية العربية للأمن السيبراني : الواقع –التحديات –الفرص، 2021
9. جامعة الدول العربية والمنظمة العربية للتكنولوجيات الاتصال والمعلومات، الاستراتيجية العربية للأمن السيبراني 2023-2027
10. مجموعة المعاهدات الأوروبية رقم 185، الاتفاقية المتعلقة بالجريمة الإلكترونية)بودابست(، 2001، https://2u.pw/LXPNcj
11. المجلس الأوروبي، المذكرة التفسيرية لاتفاقية بودابست (2001النسخة المترجمة بالعربية(، https://rm.coe.int/budapest
12. مجلس النواب الليبي، قانون رقم 5لسنة 2022م بشأن مكافحة الجرائم الإلكترونية
13. خليفة، إيهاب (2021)، الحرب السيبرانية :الاستعداد لقيادة المعارك العسكرية في الميدان الخامس)ط(1، القاهرة :العربي للنشر والتوزيع

14. رجب، إيمان (2017)، الأمن القومي العربي :تحول خريطة التهديدات والاستراتيجية المقترحة للمواجهة، معهد البحوث والدراسات العربية، القاهرة،
15. https://acpss.ahram.org.eg/News/16590.aspx
16. العمري، محمد محمود (2020)، مدخل إلى الأمن السيبراني، عمان :دار زهران للنشر والتوزيع
17. الكعبي، سليمان محمد (2018)، موسوعة استشراف المستقبل)ط(1، الإمارات العربية المتحدة :دار قنديل للطباعة والنشر والتوزيع
18. منصور، شادي عبد الوهاب (2019)، حروب الجيل الخامس :أساليب "التفجير من الداخل "على الساحة الدولية)ط(1، القاهرة :العربي للنشر والتوزيع
19. نوران، شفيق (2018)، أثر التهديدات الإلكترونية على العلاقات الدولية :دراسة في أبعاد الأمن الإلكتروني)ط(1، القاهرة :المكتب العربي للمعارف
20. الاتحاد الدولي للاتصالات (2020)، الرقم القياسي العالمي لأمن السيبراني، https://www.itu.int/ar/
21. الاتحاد الدولي للاتصالات (2015)، الرقم القياسي العالمي للأمن السيبراني وسمات السلامة السيبرانية، https://www.itu.int/ar/
22. الاجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الاتصالات 2010لمنطقة الدول العربية 19-17) يناير (2010، دمشق، سوريا
23. الأشقر، جبور منى (2016)، السيبرانية هاجس العصر، دراسات وأبحاث جامعة الدول العربية
24. الأمم المتحدة، مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، 2019
25. تقرير الاتحاد الدولي للاتصالات (2010) (ITU)، الوثيقة :RPM-ARB10/14-Aقطاع تنمية الاتصالات
26. سالم، محمد (2024)، الهجمات السيبرانية تتكثف ضد المؤسسات الاقتصادية والسياسية الليبية منذ سنتين

المراجع الأجنبية

1. ENISA ،NCSS Good Practice Guide ،Designing and Implementing National Cyber Security Strategies ،2016.
2. HM Government ،National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK.
3. Ministry of Communications and Information Technology ،Developing National Information Security Strategy for the Kingdom of Saudi Arabia ، 2011
4. Ministry of Economic Affairs and Communications ،Cybersecurity Strategy Republic of Estonia ،2019-2022.
5. Microsoft ،Developing a National Strategy for Cybersecurity: Foundations for Security and Innovation ،2013.
6. NATO Cooperative Cyber Defence Centre of Excellence ،National Cyber Security Strategy Guidelines ،Tallinn 2013
7. Organization of American States (OAS) and Global Partners Digital ، National Cybersecurity Strategies: Lessons Learned and Reflections from the Americas and Other Regions ،2022
8. Republic of Mauritius ،National Cyber Security Strategy 2012-2019

9. Global Partners ،Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers ،2020
10. The White House Washington ،The National Strategy to Secure Cyberspace ،2003
11. Kenneth Geers (2011) ،Strategic Cyber Security ،Estonia: CCD COE Publication.
12. Will Goodman (2010) ،Cyber Deterrence Tougher in Theory than in Practice (p103) ،Strategic Studies Quarterly
13. Joseph S. Nye (2010) ،Cyber Power ،Harvard Kennedy School: Belfer Center for Science and International Affairs
14. Le Nguyen, C. & Golman, W. (2021) ،Diffusion of the Budapest Convention on Cybercrime and the Development of Cybercrime Legislation in Pacific Island Countries: 'Law on the Books' vs 'Law in Action' ،Computer Law & Security Review ،40 ،105521
15. Marina Magakia (2019) ،Cyber Security and Threat Policy: The United States' Efforts to Secure the Information Age ،New York: Routledge
16. P. J. Springer (Ed.) (2017) ،Encyclopedia of Cyber Warfare ،Bloomsbury Publishing USA.
17. Thomas Rid (2013) ،Cyber War Will Not Take Place ،America: Oxford University Press
18. Tikk, Eneken and Mika Kerttunen (2020) ،Routledge Handbook of International Cybersecurity ،Routledge.

مشروعية الدليل الرقمي/ التفتيش ونطاقه؟

حكم عن القضاء الامريكي

في فبراير 1997، تلقى موظفو الجمارك في الولايات المتحدة الذين كانوا يراقبون "غرفة دردشة chat room" على شبكة الإنترنت، أثناء قيامهم بتحقيق سري undercover investigation، عددا من الصور المصورة في بوفالو بنيويورك تحتوي مواد إباحية عن الأطفال images depicting child pornography. أظهرت سجلات مزود خدمة الإنترنت أن الحاسوب الذي تم إرسال الصور منه كان مملوكا Kathi Morrissey على عنوان في كوستيجان بولاية مين. وبناء على مذكرة ضبط warrant، أجرى العملاء تفتيشا لمنزل موريسي في 21 مارس 1997.

ومن بين الأشياء التي تم الاستيلاء عليها وأخذها من المنزل جهاز الحاسوب الخاص بموريسي وعدد من الأقراص المرنة. باستخدام برامج أدوات الحاسوب computer utilities program ووظيفة "إلغاء الحذف undelete"، تمكنت الحكومة من استعادة recover حوالي 1,400 صورة محذوفة سابقا لقاصرين متورطين في سلوك جنسي صريح من القرص الصلب hard disk للحاسوب والأقراص المرنة diskettes. تضمنت هذه الصور عددا صغيرا نسبيا من الصور التي تلقاها العملاء في بوفالو في فبراير 1997 من حاسوب موريسي.

وكشف مزيد من التحقيق أنه من حوالي سبتمبر 1996 حتى مارس 1997، كان من بين سكان منزل موريسي وطفليها الصغيرين وصديقها آنذاك تروي أبهام Troy Upham. وأظهرت أدلة لاحقة، بما في ذلك اعترافات من أبهام، أن أبهام هو المستخدم الرئيسي للحاسوب وأنه كان يرسل ويستقبل المواد الإباحية المتعلقة بالأطفال عبر الإنترنت على أساس منتظم. غادر أبهام منزل موريسي إلى كندا في منتصف مارس 1997. في مايو 1997، وجهت إليه هيئة محلفين فيدرالية كبرى اتهاما، وعاد من كندا لمواجهة المحاكمة face trial.

وكما هو مبين في لائحة الاتهام ملغاة superceding indictment، اتهمت هيئة المحلفين الكبرى أبهام بأربع تهم تتعلق بنقل صور بيانية حاسوبية لقاصرين متورطين في سلوك جنسي صريح في التجارة بين الولايات انطوى إنتاجها على استخدام قاصرين متورطين في مثل هذا السلوك transporting in interstate commerce computer graphic images of minors engaged in sexually explicit conduct؛ وبنقل تجاري بين الولايات لصور بيانية حاسوبية لقاصرين متورطين في سلوك جنسي صريح؛ ويتعلق كل إحصاء بعمليات إرسال في تاريخ مختلف في فبراير 1997. انظر الباب 18 من تقنين الولايات المتحدة، 18 U.S.C. § 2252(a)(1). واتهمت التهمة الخامسة أبهام بحيازة possession 1400 صورة لقاصرين متورطين في سلوك جنسي صريح sexually explicit conduct، في "تاريخ غير محدد" ولكن بين 7 فبراير 1997 و21 مارس 1997، والتي تضمن إنتاجها استخدام قاصرين متورطين في مثل هذا السلوك. انظر الباب 18 من تقنين الولايات المتحدة، 18 U.S.C. § 2252(a)(4)(B).

تأكيدا على العديد من الأسباب، قدم Upham طلبا لرفض suppress الأدلة المستمدة من تفتيش منزل موريسي. وفي 11 أغسطس 1997، عقدت المحكمة المحلية جلسة استماع بشأن الأدلة بشأن الطلب. ورفضت محكمة المقاطعة الطلب، وتم قبول الصور المستمدة من البحث- التي تم التقاطها من حالتها المحذوفة- في وقت لاحق في المحاكمة. ونؤجل في الوقت الحالي وصفا للأسباب التي قدمها الآن Upham لتبرير الرفض suppress وردود الحكومة على تلك الادعاءات.

تمت محاكمة أبهام من قبل هيئة محلفين في محاكمة استمرت ثلاثة أيام أجريت في سبتمبر 1997، وقدمت الحكومة أدلة على الصور التي تم تلقيها في بوفالو من حاسوب موريسي وتلك التي تم استردادها من القرص الصلب للحاسوب والأقراص التي تم الاستيلاء عليها في البحث. كما قدمت أدلة تربط Upham بإرسال الصور واستلامها. وأخيرا، أدلى طبيب بشهادته للحكومة لتقديم أدلة طبية على أعمار الأطفال الذين تم تصويرهم في الصور.

وأدلى أبهام بأقواله في المحاكمة دفاعا عن نفسه لكنه لم ينكر إرسال واستقبال المواد الإباحية للأطفال عبر الإنترنت. وبدلا من ذلك، جادل أبهام بأنه تعرض للاعتداء الجنسي عندما كان طفلا وأن تبادله لمثل هذه الصور على الإنترنت مع مشاركين آخرين في "غرفة الدردشة chat room" تم فيما يتعلق بإعداده لكتاب جاد يتعلق بإساءة معاملة الأطفال. وقال إنه كتب عددا صغيرا من الصفحات، وإن كان ذلك على مدى فترة طويلة جدا، كجزء من هذا المشروع.

ولقد أدانت convicted هيئة المحلفين أبهام في جميع التهم الخمس. وأعطيت هيئة المحلفين استجوابا منفصلا separate interrogatory للرد عليه إذا أدانت بتهمة واحدة أو أكثر: "هل كان الغرض الوحيد للمتهم defendant في ارتكاب الجريمة أو الجرائم هو إنتاج عمل أدبي جاد؟" أجابت هيئة المحلفين بالنفي. في الوقت المناسب، حكم على أبهام بالسجن لمدة 78 شهرا، وهو الحد الأدنى الذي توفره إرشادات إصدار الأحكام على الجرائم في ضوء التاريخ الإجرامي السابق prior criminal history لأبهام.

ويستأنف أبهام الآن، ويثير مجموعة واسعة من القضايا في مذكرة قدمها المحامي وفي ملحق أعده أبهام نفسه. ومن بين هؤلاء، فإن الشيء الوحيد الذي يتطلب مناقشة كاملة هو ادعاء Upham متعدد الأجزاء بأن اقتراح الإلغاء كان يجب أن يمنح. وعلى وجه الخصوص، يقول أبهام إن المذكرة كانت واسعة للغاية وأن نطاقها تم تجاوزه عندما استعادت الحكومة من القرص الصلب والأقراص المرنة الصور التي تم حذفها سابقا.

وفي البداية، ان اعتراض الحكومة على أن Upham ليس لديه اساس للطعن في البحث. وهذا هو الحال، كما تقول، لأن أبهام اعترف الآن بأنه انفصل عن موريسي وانتقل في 13 مارس 1997، قبل حدوث التفتيش before the search occurred، وبالتالي كان يفتقر إلى أي اهتمام بالخصوصية في المبنى therefore lacked any privacy interest in the premises[1]. وتقر الحكومة بأنها لم تقدم هذه الحجة في محكمة المقاطعة. ومن المحتمل جدا أنه لم يكن لديها ما يعتبر الآن اعترافا واضحا من Upham، أي أنه عندما انتقل إلى كندا، لم يكن ينوي العودة إلى منزل موريسي.

على الرغم من أن الحكومة قد تنازلت عن الحجة الدائمة، فلا شيء يمنعنا من النظر فيها إذا اخترنا القيام بذلك، على افتراض أن هذا لن يكون غير عادل لـــ Upham، انظر قضية United States v. Pervaz [2] وفي هذه الحالة نعتقد أنه لن يكون عادلا. على الرغم من بعض الأدلة على الانفصال، فإن السجل ليس

[1] See Rakas v. Illinois, 439 U.S. 128, 131 n. 1, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978)
[2] Cf. United States v. Pervaz, 118 F.3d 1, 4 (1st Cir.1997).

واضحا لدرجة تمنع Upham من المجادلة (والشهادة بالفعل) بأنه خطط للعودة أو كان له صلة أخرى متبقية بالممتلكات. والمكان المناسب لتسوية هذه القضايا هو جلسة رفض الدليل suppression hearing.

أول طعن لأبهام في مذكرة الضبط warrant في هذه المحكمة هو أنها كانت عامة في وصفها لما كان سيتم عليه الضبط seized ولم تستوف الاختبارات المفترضة لمثل هذا الأمر. وأرفق الأمر نفسه قائمة بالمواد التي يتعين مصادرتها والتي أدرجت في طلب إصدار أمر الاعتقال، وأدرجها بالإحالة. وكان البندان الأولان في القائمة - العنصران الوحيدان اللذان لهما صلة مباشرة هنا - على النحو التالي:

Any and all computer software and hardware, . computer disks, disk drives.

جميع برامج وأجهزة الحاسوب computer software and hardware، وأقراص الحاسوب disks، ومحركات الأقراص disk drives.

Any and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute].

جميع الصور المرئية، بأي شكل أو وسائط، للقاصرين الذين ينخرطون في سلوك جنسي صريح [على النحو المحدد في القانون].

وتقول الحكومة إن أيا من الفقرتين ليست معيبة. وتقول الحكومة أيضا إن هجوم أبهام على مذكرة التوقيف باعتباره عاما جدا لم يتم إجراؤه في اقتراح الرفض وأن أبهام يقتصر بالتالي على الخطأ البسيط في هذه المسألة. ويبدو أن الحكومة محقة فيما يتعلق بالتنازل waiver، ولكن نظرا لأننا نعتقد أنه لم يكن هناك خطأ على الإطلاق، فإننا نفضل معالجة الأمر بهذه الشروط من أجل تقديم إرشادات بشأن ما قد يكون مشكلة متكررة.

إن مسألة ما إذا كان الأمر "خاصا particular" بما فيه الكفاية قد تم التقاضي بشأنها كثيرا مع نتائج متباينة على ما يبدو. انظر الاستعراض السنوي السادس والعشرون للإجراءات الجنائية[3]. والاساس هو اتجاه التعديل الرابع بأن المذكرة تصف "على وجه الخصوص particularly" المكان place الذي سيتم تفتيشه و"الأشخاص أو الأشياء التي سيتم الضبط عليها persons or things to be seized"[4]. وينشأ شرط الخصوصية requirement of particularity من العداء لممارسة التاج Crown's practice (اعلى

[3] See Twenty-Sixth Annual Review of Criminal Procedure, 85 Geo. L.J. 821, 836-38 & nn. 75-78 (1997)(collecting cases).
[4] U.S. Const. amend IV.

السلطات) المتمثلة في إصدار "أوامر عامة general warrants" تتخذ للإذن بالتفتيش بالجملة في ممتلكات شخص ما بحثا عن مواد مهربة أو أدلة[5].

وتتعلق القضايا المتعلقة بـ.. "الخصوصية particularity" في الواقع بمشكلتين مختلفتين على الأقل: الأولى هي ما إذا كانت مذكرة الضبط توفر معلومات كافية لتوجيه ومراقبة حكم مأمور الضبط في اختيار ما يجب اتخاذه[6]، والأخرى هو ما إذا كانت الفئة المحددة واسعة جدا بمعنى أنها تشمل البنود التي لا ينبغي الاستيلاء عليها[7]، ولسوء الحظ، فإن جعل الأمر أكثر موضوعية قد يجعله أوسع، والعكس صحيح vice versa.

ان هجوم Upham الرئيسي هو على الفقرة الأولى، مما يسمح بالاستيلاء على معدات الحاسوب، والتي يصفها بأنها "عامةgeneric ". وعلى الرغم من أن Upham يعتمد بشكل أساسي على قضية الولايات المتحدة ضد كلين[8]. حيث كانت تلك القضية تتعلق بما إذا كان الأمر غير دقيق لأنه يسمح بإصدار أحكام ذاتية لا مبرر لها. وهنا، يمكن بسهولة إدارة الفقرة الأولى استنادا إلى معايير موضوعية (أي ما إذا كانت الأصناف المضبوطة معدات حاسوبية). والمشكلة ليست عدم الدقة ولكن تجعل الجدل يكثر ويتسع.

ومن الناحية العملية، كان الاستيلاء على الحاسوب وجميع الأقراص المتاحة وتفتيشها لاحقا خارج أماكن العمل يتعلق بأضيق عملية بحث وضبط يمكن تعريفها ومن المرجح بشكل معقول الحصول على الصور. تم تحديد فرصة كافية للعثور على بعض الإبر في كومة قش الحاسوب من خلال السبب المحتمل probable-cause الذي يظهر في طلب الأمر؛ والتفتيش في جهاز حاسوب وأقراص مشتركة ليس بطبيعته أكثر تدخلا من التفتيش المادي لمنزل بأكمله بحثا عن سلاح أو مخدرات. ونختتم، كما فعلت الدائرة التاسعة في ظروف مماثلة إلى حد ما، أن انظر قضية Lacy [9] ، حيث أن الفقرة الأولى لم تكن فضفاضة بشكل غير دستوري unconstitutionally overbroad.

وبطبيعة الحال، لو كان من السهل الحصول على الصور نفسها من خلال تفتيش الموقع site inspection، فربما لم يكن هناك مبرر للسماح بمصادرة جميع المعدات الحاسوبية، وهي فئة يحتمل أن تشمل معدات لا تحتوي على صور ولا صلة لها بالجريمة. ولكن ليس من السهل البحث في محرك أقراص ثابت محمل جيدا من خلال تصفح جميع المعلومات التي يحتوي عليها، ناهيك عن البحث من خلاله والأقراص عن المعلومات التي ربما تم "حذفها deleted". ويظهر السجل أن آليات البحث عن الصور التي أجريت لاحقا خارج الموقع لم يكن من الممكن إجراؤها بسهولة على الفور.

---

[5] See Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971).

[6] see United States v. Abrams, 615 F.2d 541, 545-46 (1st Cir.1980);
[7] see United States v. Kow, 58 F.3d 423, 427 (9th Cir.1995). See also Davis v. Gracey, 111 F.3d 1472, 1478-79 (10th Cir.1997) (discussing both problems).
[8] United States v. Klein, 565 F.2d 183, 188 (1st Cir.1977).
[9] see United States v. Lacy, 119 F.3d 742, 746-47 (9th Cir.1997).

وتجادل الحكومة، بدلا من ذلك، بأن الفقرة الثانية، التي تسمح بالاستيلاء على الصور غير القانونية، تبرر وحدها الاستيلاء على المعدات بغض النظر عن الفقرة الأولى. ويدعي أبهام أن الفقرة الثانية ليست أيضا "خاصة" بما فيه الكفاية ولكنه يفعل ذلك عن طريق اقتباس الفقرة بشكل خاطئ واعتراضه غير مقنع objection is unpersuasive[10]. ثم ان قلقنا من الحجة البديلة alternative argument للحكومة هو قلق مختلف، وهو ما نلاحظه دون السعي إلى حل المشاكل الصعبة المطروحة على هذا النحو.

وما من شك في أن الأمر الذي لا يتضمن سوى الفقرة الثانية سيسمح بتفتيش أية "حاوية container" قد يكون من المعقول إخفاء الصور "من الداخل inside" - بما في ذلك الحاسوب وأي أقراص[11].

ومع ذلك، هناك بعض الانقسام في السوابق القضائية case law بشأن ما إذا كان يجوز للشرطة أن تصادر وتزيل من أماكن العمل أشياء لم يرد اسمها في الأمر لمجرد الأمل المعقول reasonable hope في أن يؤدي تفتيش تلك الأشياء في وقت لاحق إلى استعادة الأشياء التي تم تسميتها[12]. حيث تقوم الشرطة بسحب محتويات المنزل بالكامل، بما في ذلك الثلاجة، لأغراض التفتيش في وقت لاحق.

وتنشأ هذه المشكلة في مجموعة متنوعة من السياقات المختلفة وفي العديد من التبادلات permutations. ويتعلق الأمر بمسائل تتعلق بالدرجة وربما لا توجد قاعدة واحدة تحل جميع هذه الحالات. وفي هذه الحالة، ليس من الضروري البت فيما إذا كان يمكن تبرير نقل المعدات الحاسوبية computer equipment بالفقرة الثانية فقط لأن الفقرة الأولى تأذن بوضوح بضبط المعدات، مما يسمح بإخراجها من الموقع. وما إذا كان البحث اللاحق خارج الموقع عن الصور يمثل أية مشكلة هو الموضوع الذي ننتقل إليه بعد ذلك.

ان ادعاء Upham الرئيسي الثاني للخطأ هو أن استعادة المعلومات المحذوفة مسبقا recovery of previously deleted information على القرص الصلب والأقراص المرنة كانت خارج نطاق المذكرة outside the scope of the warrant. ومن المستقر عليه قانونا أن التفتيش والضبط search and

---

[10] He treats the paragraph as if it authorized the seizure of any image and ignores the qualifying language limiting the seizure to images "of minors engaging in sexually explicit conduct." Such language has been held to leave "little latitude" to the executing officers and to be sufficiently particular to satisfy the Fourth Amendment. See, e.g., United States v. Kimbrough, 69 F.3d 723, 727-28 (5th Cir.1995); United States v. Peden, 891 F.2d 514, 517 (5th Cir.1989); United States v. Hurt, 808 F.2d 707, 707 (9th Cir.1987).

[11] See United States v. Ross, 456 U.S. 798, 820-22, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982); United States v. Giannetta, 909 F.2d 571, 577 (1st Cir.1990).

[12] Compare United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir.1997) (seizure of entire file cabinet including intermixed warrant-specified and unspecified documents permissible); United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir.1991) (same); United States v. Shilling, 826 F.2d 1365, 1369-70 (4th Cir.1987) (same); United States v. Johnson, 709 F.2d 515, 516 (8th Cir.1983) (subsequent off-site search of safe did not require owner's consent when safe could properly be searched on-site), with United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir.1982) (subsequent search of intermixed warrant-specified and unspecified documents that were seized wholesale requires further approval of magistrate).

seizure اللذين يجريان بموجب أمر قضائي يجب أن يتفقا مع الأمر[13]، وهنا، فان حجة Upham ذات شقين: أن الأمر لم يأذن بتفتيش الحاسوب على الإطلاق، وأنه لم يأذن بإلغاء حذف المعلومات/ البيانات المحذوفة مسبقا authorize the undeleting of previously deleted information.

الفرع الأول من الحجة ميؤوس منه hopeless. والأمر warrant اتاح صراحة ضبط كل من الحاسوب والأقراص المرنة والصور غير القانونية. والصور- التي نتجاهل سؤال الحذف deletion question في الوقت الحالي- كانت "داخل" الحاسوب أو الأقراص المرنة. لذلك تم التفكير في استخراج صور غير قانونية من داخل الحاسوب والأقراص المرنة بموجب أمر السماح بتطوير فيلم غير مطور تم الاستيلاء عليه بموجب أمر قضائي دون اشتراط أمر إضافي[14]؛ (فقد رفض القضاء السماح بالمعالجة المختبرية لبقع الدم التي تم جمعها في تفتيش قانوني دون أمر إضافي).

الفرع الآخر والأكثر خطورة من الحجة هو التحدي لاستعادة المواد المحذوفة[15]. من على الأقراص المرنة، فقد استعادت الحكومة الصور ببساطة باستخدام وظيفة إلغاء الحذف للحاسوب. ومع ذلك، تمت إعادة تهيئة القرص الصلب بواسطة Upham في 8 مارس 1997، وهي عملية تمحو بعض رموز الفهرسة التي تسمح بإلغاء الحذف بسرعة. ولكن حتى يتم استبدال المعلومات المحذوفة فعليا بمعلومات جديدة، يمكن في كثير من الأحيان استرداد المعلومات القديمة بواسطة برنامج فائدة متخصص، وهو ما فعلته الحكومة في هذه الحالة.

ان ضبط seizure الصور غير القانونية unlawful images كان في حدود اللغة الواضحة للمذكرة. ولا يختلف استعادتها recovery، بعد محاولة التدمير attempted destruction، عن فك تشفير رسالة مشفرة تم الاستيلاء عليها بشكل قانوني decoding a coded message lawfully seized أو لصق قصاصات من مذكرة فدية ممزقة pasting together scraps of a torn-up ransom note[16]. حيث لم ينص أمر 21 مارس على طرق التعافي أو الاختبارات التي يتعين إجراؤها، لكن أوامر الاعتقال نادرا ما تفعل ذلك.

---

[13] see Marron v. United States, 275 U.S. 192, 196-97, 48 S.Ct. 74, 72 L.Ed. 231 (1927), or some well-recognized exception. E.g., Horton v. California, 496 U.S. 128, 130, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990); United States v. Robles, 45 F.3d 1, 6-7 (1st Cir.), cert. denied, 514 U.S. 1043, 115 S.Ct. 1416, 131 L.Ed.2d 300 (1995) (plain view seizures).

[14] See, e.g., State v. Petrone, 161 Wis.2d 530, 468 N.W.2d 676, 681 (Wis.1991) (permitting development of undeveloped film seized pursuant to a warrant without requiring additional warrant); State v. Warren, 309 N.C. 224, 306 S.E.2d 446, 449 (1983) (permitting lab processing of bloodstains gathered in a lawful search without additional warrant).

[15] We reject the government's suggestion that, by deleting the images, Upham "abandoned" them and surrendered his right of privacy. Analogy is a hallowed tool of legal reasoning; but to compare deletion to putting one's trash on the street where it can be searched by every passer-by, see California v. Greenwood, 486 U.S. 35, 40, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988); United States v. Scott, 975 F.2d 927, 930 (1st Cir.1992), is to reason by false analogy.

[16] See Commonwealth v. Copenhefer, 526 Pa. 555, 587 A.2d 1353, 1356 (1991); cf. Petrone, 468 N.W.2d at 681.

وتتعلق عملية الأمر في المقام الأول بتحديد ما يمكن تفتيشه أو مصادرته- وليس كيف- وما إذا كان هناك سبب كاف لانتهاك الخصوصية على هذا النحو.

وننتقل الآن، وبإيجاز، إلى موضوع مختلف تماما. لدى Upham زوج من الحجج ذات الصلة، واحدة موجهة إلى كفاية الأدلة والأخرى إلى تعليمات هيئة المحلفين. وكلاهما يعتمد على التأكيد على أنه لا يمكن إدانة أبهام بشكل صحيح لمعرفته بحيازة صور غير قانونية يعتقد أنه تم حذفها من الحاسوب والأقراص المرنة وربما لم يكن يعلم أنه يمكن استعادتها.

لم يعرض Upham هذه القضايا على المحكمة الابتدائية. وقد طلب بالفعل إصدار حكم بالبراءة ولكنه لم يثر هذا الطلب أو الاعتراض. وقد قدم اعتراضات على التعليمات ولكن ليس تلك التي تم الضغط عليها الآن. ويتم التنازل عن كفاية الاعتراضات على الأدلة، إذا لم يتم تقديمها أدناه، إلا عند الضرورة لتجنب الظلم injustice "الواضح والجسيم clear and gross"[17].

وفي هذه الحالة، نحن مقتنعون بأن الأخطاء المزعومة المشكو منها الآن لم يكن لها أي تأثير على الحكم وبالتالي فشلت في اختبار الخطأ العادي plain error test [18]. وأظهرت الأدلة بأغلبية ساحقة overwhelmingly أن المتهم أبهام نقل عن علم صورا غير قانونية وتلقاها وحازها قبل محاولة حذفها؛ كانت الصور المعاد استعادتها دليلا مؤهلا تماما على الجرائم المرتكبة قبل حذفها. ولم تعتمد الإدانة على السؤال (الذي لا نقرره) حول ما إذا كان من غير القانوني بمفرده امتلاك قرص صلب أو أقراص مرنة تحتوي على صور محذوفة (ولكن قابلة للاستعادة recapturable)، مع المعرفة المطلوبة requisite knowledge.

وأخيرا، يعترض أبهام في طعن الحكم الصادر ضده بأن قاضي المقاطعة district judge رفض منح أبهام تعديلا تنازليا لقبول المسؤولية[19]. حيث يدرك المتهم أبهام أنه نادرا ما يسمح بالتعديل adjustment عندما يرفض المتهم الاعتراف بالذنب where the defendant declines to plead guilty [20]، لكنه يقول إنه في هذه الحالة لم يطعن في الحيازة وأصر على المحاكمة فقط لتقديم دفاعه "التعديل الأول".

كما ان "قبول المسؤولية Acceptance of responsibility" غير معرف بشكل مجرد في المبادئ التوجيهية guidelines. وبدلا من ذلك، يتم تنقيح المفهوم بسلسلة من التعليقات[21]، ويربط أحد التعليقات التخفيض بشكل وثيق بالإقرار بالذنب، قائلا إنه "نادرا rarely" فقط ما يتم منح التعديل لمن يصر على

---

[17] see United States v. Greenleaf, 692 F.2d 182, 185 (1st Cir.1982), cert. denied, 460 U.S. 1069, 103 S.Ct. 1522, 75 L.Ed.2d 946 (1983); and failure to object or make a proper request at the instruction stage is fatal except for plain error. See United States v. Campbell, 874 F.2d 838, 841 (1st Cir.1989).

[18] See United States v. Olano, 507 U.S. 725, 732, 113 S.Ct. 1770, 123 L.Ed.2d 508 (1993).
[19] See U.S.S.G. § 3E1.1.
[20] see id. app. note 2.
[21] see U.S.S.G. § 3E1.1, app. notes 1-6.

المحاكمة، مضيفا أنه حتى الإقرار بالذنب لا يضمن التخفيض. ومع ذلك، يقول نفس التعليق إنه حتى المتهم الذي يصر على المحاكمة "قد may" يظهر قبولا في حالات نادرة، وهذا يوضح هذه النقطة:

وقد يحدث ذلك، على سبيل المثال، عندما يذهب المتهم إلى المحاكمة لتأكيد وحفظ المسائل التي لا تتعلق بالذنب الفعلي (على سبيل المثال، لتقديم طعن دستوري constitutional challenge في تشريع statute أو طعن في انطباق تشريع على سلوكه (applicability of a statute Id).

.

يمكن القول إن الاتجاه الرئيسي للدفاع عن المتهم أبهام في المحاكمة كان ادعائه بأنه كان يمتلك مواد إباحية للأطفال من أجل تأليف كتاب عنها. وقد يكون الذهاب إلى المحاكمة فقط لتقديم هذا الدفاع المزعوم يقع ضمن روح/ حكمة، إن لم يكن نص، التعليق التوجيهي المقتبس للتو. ولكن التعليق لا يفعل أكثر من مجرد إزالة حاجز واحد أمام التعديل. وتؤكد اللغة المحيطة في التعليق، والغرض من إتاحة التعديل، أنه لا يزال يتعين على المتهم أن يظهر بشكل إيجابي أنه "يقبل المسؤولية accept responsibility" عن جريمته offense [22].

هنا، حكم قاضي المقاطعة بأن الفرضية الواقعية factual premise للدفاع كانت غير صحيحة untrue، مشيرا إلى استنتاج هيئة المحلفين بأن سلوك أبهام لم يكن مدفوعا فقط بالطموح الأدبي. وهذا الحكم ليس "خاطئا بشكل واضح clearly erroneous"، وهو المعيار الطبيعي للمراجعة[23]. وبالتأكيد، تشير الأدلة بقوة إلى استنتاج مفاده أنه مهما كانت دوافع أبهام متشابكة، فإن الإشباع الجنسي كان هدفا مركزيا لأفعاله. وعلى مدى سنوات عديدة من كتابة الكتب المزعومة، كتب أبهام بضع صفحات فقط من هذا العمل المفترض.

قد يكون من المبالغة في التبسيط oversimplification أن نقول (بعد فرويد Freud) أن أبهام يجب أن يكون "يكذب بوعي consciously lying" في المحاكمة بشأن دوافعه الخاصة. ولكن المتهم الذي يقدم شهادة زور false testimony في المحاكمة، في محاولة لتقليل ذنبه culpability، ليس في وضع يسمح له بالإصرار على أن يمنحه القاضي تخفيضا لقبول المسؤولية[24]. وفي جميع الأحوال، لم تتجاوز محكمة المقاطعة district court في هذه القضية "التمييز الكبير great deference " الممنوح للقاضي الذي أصدر الحكم في تقييم ادعاءات قبول المسؤولية responsibility [25].

تم النظر في مطالبات أخرى قدمت نيابة عن Upham (على سبيل المثال، الادعاء بأن محكمة المقاطعة أخطأت في العثور على واحدة أو أكثر من الصور كانت سادية مازوشية/ سادية جنسية sadomasochistic وبالتالي تبرر تعديلا تصاعديا upward adjustment)، ولكنها لا تتطلب مناقشة منفصلة. ومن الواضح أن العقوبة شديدة ولكن هذا يرجع جزئيا إلى التعديلات التصاعدية، مثل تلك المذكورة للتو، والتاريخ الجنائي

[22] See also U.S.S.G. § 3E1.1(a); United States v. Lombard, 72 F.3d 170, 187 (1st Cir.1995).
[23] See United States v. Ocasio-Rivera, 991 F.2d 1, 4 (1st Cir.1993).
[24] See U.S.S.G. § 3E1.1 app. note 1(a).
[25] Id. app. note 5.

السابق الهام significant prior criminal history، بما في ذلك إدانة سابقة باستغلال الأطفال في المواد الإباحية child-pornography conviction بموجب قانون الولاية.

تم التأكيد Affirmed

بودين، قاضي الدائرة .BOUDIN, Circuit Judge

المصدر

https://caselaw.findlaw.com/us-1st-circuit/1176381.html

التطور المفاهيمي من التوعية إلى إدارة المخاطر البشرية في الأمن السيبراني

إعداد

م. سمر ميلود الدبري

رئيس قسم التوعية والعلاقات بالهيئة الوطنية لأمن وسلامة المعلومات

بكالوريوس: تحكم آلي

طالبة دراسات عليا / ماجستير – تخصص دراسات المعلومات

الأكاديمية الليبية للدراسات العليا .

الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority

الملخص(Abstract)

يهدف البحث إلى إعادة تعريف التوعية بالمخاطر السيبرانية كمفهوم أصيل من مفاهيم الأمن السيبراني ارتبط بها ارتباط الإنسان باستخدام التقنية ، والتعامل معها و التأثير فيها و التأثر بها ، وكونها جزءاً لا تجزأ من سلسلة التأمين سواء على مستوى الفرد أو على مستوى المؤسسات و التي اعتبر فيها الإنسان على الدوام الحلقة الأضعف كما يوصف في أغلب الأدبيات التي تتحدث عن هذا الجانب ، كما يهدف إلى إدخال مفهوم حديث نسبياً حول التعامل مع الحلقة الأضعف و إضفاء جوانب إنسانية على التكنولوجيا ، وعدم إغفال السلوكيات البشرية التي تؤدي إلى خطر أمني محتمل ، وصولاً إلى كيفية إدارة هذه السلوكيات للتقليل من المخاطر السيبرانية في بيئة العمل .

اعتمدت هذه الدراسة المنهجية النظرية التي تقوم على مراجعة وتحليل الأدبيات والبحوث العلمية السابقة المتعلقة بإدارة المخاطر البشرية في الأمن السيبراني. تم التركيز على بناء إطار مفاهيمي من خلال استعراض نقدي للنماذج والتوجهات الحديثة في الأدبيات، دون استخدام أدوات أو نتائج ميدانية. والتي من الممكن تناولها مستقبلاً.

الكلمات المفتاحية(Keywords)

إدارة المخاطر البشرية، الأمن السيبراني ، التوعية ، العوامل البشرية ، التهديد الداخلي.

المقدمة

أصبح من المسلم به أن للأمن السيبراني أهمية قصوى في حماية المؤسسات من الهجمات السيبرانية التي تؤثر على سمعتها وسمعة موظفيها ووضعها المالي، وعلاقاتها مع باقي المؤسسات، وثقة عملاءها.. فأنظمة الأمن السيبراني لها دور حيوي في منع / تقليل التهديدات المؤدية لتسرب البيانات وسرقتها وحتى التعديل عليها مما يمس بسريتها وتكاملها وتوافرها وهي ثالوث أمن المعلومات الذي تبنى عليه استراتيجيات وحلول الأمن السيبراني لحماية المعلومات والأصول الرقمية داخل المؤسسات سواء كانت تلك المعلومات شخصية أو مالية أو ملكية فكرية أو غيرها..

وهنا يمكن طرح تساؤل هام من هو المستفيد من الأمن السيبراني ومن هو المتضرر ومن سينفذ الحلول ويطبق استراتيجية الحماية والدفاع، ولمن تؤول الحقوق التي ستنتهك بتهديد سيبراني، ومن هو المسؤول عن حماية الأصول الرقمية للمؤسسة للوصول إلى إجابة واحدة تتمحور حول العنصر البشري أو ما يطلق عليه العامل البشري .Human Factor

وقد زاد تأثير العامل البشري في الأمن السيبراني بشكل كبير بسبب الزيادة المضطردة في استخدام التقنية وانتشار واسع للخدمات السحابية التي تخزن معلومات حساسة قد يستهدفها مجرمو الانترنت.. وفي المقابل تتطور مع هذا الاضطراد في الاستخدام أساليب الهجوم بأدوات وتقنيات متقدمة.

لذا فعملية التأمين والحماية لا تقتصر فقط على الجانب التقني، بل هي تثقيف وتوعية لمستخدم التقنية لتعزيز وعي الأفراد بمخاطر الأمن السيبراني وكيفية التعامل معها للتقليل من فرص وقوع المستخدم في موقع المتسبب بالضرر.. ويمكن أن نلخص أهمية الأمن السيبراني في ظل تنامي التهديدات البشرية فيما يلي:

- حماية البيانات الحساسة والملكية الفكرية.
- تقليل مخاطر الاختراق والهجمات الإلكترونية المتطورة.
- تعزيز وعي وتثقيف الموظفين لعناصر خطر أقل من الأخطاء البشرية.
- ضمان استمرارية الأعمال وتقليل الخسائر المالية.
- الامتثال للمتطلبات التنظيمية والقانونية.
- المحافظة على سمعة المؤسسة وثقة العملاء.

هذه العوامل مجتمعة توضح كيف أن الأمن السيبراني عنصر لا غنى عنه في البيئة الرقمية المعاصرة، خصوصًا مع تزايد التهديدات التي تنبع من العنصر البشري سواء المقصود منه أو الذي دون قصد.

مشكلة البحث

في ظل التطورات المتسارعة والتهديدات المتزايدة في مجال الأمن السيبراني، أصبحت برامج التوعية الأمنية التقليدية التي تعتمد على تقديم المعلومات فقط للمستفيدين مجرد مصطلح يوحي بأثر نفسي سلبي، إذ يمنح المتلقي دورًا محدودًا ومرتبطًا بالتعلم السلبي بدلاً من المشاركة الفاعلة في حماية البيئة السيبرانية. هذا

النمط من التوعية لا يعكس الطموح الحقيقي نحو تعزيز الأمن داخل المؤسسات، حيث يظل الموظف متلقياً لا فاعلاً أو مبادراً.

إن التحدي الحقيقي يكمن في الارتقاء من مفهوم التوعية الذي يركز فقط على نشر المعرفة السيبرانية ومشاركتها وتقييمها تبعاً لنضج المؤسسة، إلى تبني منهج إدارة المخاطر البشرية الشامل الذي يمكّن الموظف ويجعله شريكاً فعالاً في منظومة الحماية السيبرانية. إذ أن الأمن السيبراني الحالي يتطلب مشاركة نشطة وتقييم مستمر للسلوك البشري، وتحليل البيانات المتعلقة بالمخاطر التي يحملها العنصر البشري، إلى جانب دمج التدابير التقنية مع السياسات التوعوية والثقافية المتطورة.

وبالتالي، لم تعد التوعية الأمنية التقليدية كافية في ظل الهجمات المعقدة مثل الهندسة الاجتماعية التي تستهدف الثقة والسلوك البشري، مما يتطلب إعادة النظر في تصميم برامج الأمن السيبراني لتشمل آليات تمكينية ديناميكية تزيد من التفاعل وتحول الموظفين من مجرد متلقين إلى صناع قرار ودرع حماية فعليين. ومن هنا يمكن طرح بعض التساؤلات:

1. هل يمثل التطور من برامج التوعية إلى إدارة المخاطر البشرية تحسناً في المفهوم المؤسسي للأمن السيبراني ويستلزم استراتيجيات متكاملة تشمل العنصر البشري؟
2. هل تعزز إدارة المخاطر البشرية فعالية الأمن السيبراني مقارنة بالاعتماد على برامج التوعية فقط، وفقًا لمراجعة الأدبيات العلمية؟
3. هل توجد فجوة في تطبيق الممارسات بين التوعية الأمنية التقليدية وإدارة المخاطر البشرية داخل المؤسسات، كما تشير إليها الدراسات الحديثة؟
4. إلى أي مدى تركز الأدبيات الحديثة على دمج التقنيات الحديثة مع منهجيات إدارة المخاطر البشرية لتعزيز الحماية السيبرانية؟

المنهجية

استخدمت في البحث المنهج الوصفي لمناسبته لطبيعته التي تهتم بجمع المعلومات المتعلقة بالاتجاهات الحديثة في التعامل مع المخاطر البشرية في مجال الأمن السيبراني، والأسس النظرية التي ترتكز عليها، واستخلاص بعض المعلومات التي يمكن الإفادة منها في تطوير أساليب التعامل مع العامل البشري في المجال.

وقد تم جمع البيانات باستخدام أسلوب أداة المراجعة الأدبية للمؤلفات الحديثة التي تتحدث عن مفهوم ودور العامل البشري في مجال الأمن السيبراني والتركيز على الجزء المتعلق بأهمية العمل على تطوير المفاهيم النظرية المتعلقة بالتوعية إلى ما بعدها من إدارة للمخاطر البشرية في اتجاه دراسة وتوجيه السلوكيات الغير آمنة لتكون سلوكيات أكثر أماناً مع القيام بالتدخلات اللازمة في حال انحراف السلوك عن المسار المطلوب أمنياً.

مراجعة بعض الأدبيات (Literature Review)

في تقرير ENISA الصادر عام 2016 بعنوان "تعريف الأمن السيبراني: الفجوات والتداخلات في التوحيد القياسي"، تم الإشارة إلى غياب تعريف موحد عالمي للأمن السيبراني، حيث تتفاوت التعريفات بين الباحثين بناءً على عدة عوامل، منها طبيعة العناصر التي يتم حمايتها، ونوعية التهديدات، وما إذا كانت الأخطاء غير المقصودة ضمن نطاق التعريف أم لا. غالبًا ما تركز التعريفات التقليدية، مثل تعريف قاموس أكسفورد، على الحماية من الهجمات الخارجية، حيث يُعرف الأمن السيبراني بأنه حالة حماية البيانات الإلكترونية من الاستخدام غير المصرح به أو الإجرامي.

من جهة أخرى، يقدم المعيار الدولي ISO/IEC تعريفًا أكثر شمولًا يصف الأمن السيبراني بأنه الحفاظ على سرية وتكامل وتوافر المعلومات في الفضاء الإلكتروني. هذا التعريف القائم على مبادئ "السرية، والتكامل، والتوافر" (CIA) يتيح إدراك الدور الحيوي للبشر في كل من التهديدات الأمنية والحماية منها، دون أن يقتصر فقط على المخاطر التقنية.

ومع ذلك، فإن هذا التعريف قد يقلل من أهمية المخاطر الفيزيائية، مثل التخريب المتعمد للمكونات الحيوية للبنية التحتية، أو استخدام الفضاء السيبراني لأغراض جمع المعلومات الاستخباراتية، والتي قد تكون جزءًا من التهديدات الأمنية المعقدة. (1)

عند الربط مع مفهوم المخاطر البشرية في الأمن السيبراني، نلاحظ أن التعريفات التقليدية والعملية الأمنية قد تميل غالبًا إلى التركيز على العوامل التقنية أو الخارجية، في حين أن العنصر البشري يشكل أحد أهم مصادر المخاطر الأمنية. هذه المخاطر البشرية تتضمن الأخطاء غير المقصودة مثل الإهمال أو سوء الاستخدام، وكذلك التهديدات المتعمدة عبر الهندسة الاجتماعية أو سوء استخدام الصلاحيات..

لذلك، من الضروري توسيع فهم وتعريف الأمن السيبراني بالنسبة للمؤسسات بحيث يشمل الجانب البشري بشكل واضح، باعتباره عاملاً حيويًا يؤثر على سرية وسلامة وتوافر الأنظمة والمعلومات، ولذا فإن إدارة المخاطر البشرية وضمان وعي الأفراد وتدريبهم تشكل حجر الزاوية في تعزيز أمن الفضاء السيبراني بشكل شامل ومستدام.

المحور الأول: التوعية بمخاطر الأمن السيبراني

مفهوم التوعية بمخاطر الأمن السيبراني (التوعية السيبرانية)

تعتبر التوعية السيبرانية جزءاً من الآليات الغير تقنية التي تهدف إلى تحقيق متطلبات الأمن السيبراني، ويمكن تعريفها حسب المعهد الوطني للمعايير والتقنية بالولايات المتحدة الأمريكية NIST (National Institute of Standards and Technology على أنها تمثل مجموعة الحملات التي تستخدم جميع الوسائل الممكنة لجذب اهتمام المستهدفين وتوجيه تركيزهم نحو الأمن السيبراني وأهميته بهدف جعلهم مدركين للمخاوف وا لأخطار والتهديدات الأمنية والوقاية منها والتعامل معها بالطرق السلمية.(2)

ووفقاً لمعهد(2017) SANS ، تُعرف التوعية السيبرانية بأنها عملية مستمرة تهدف إلى تعزيز فهم الأفراد للمخاطر والتهديدات السيبرانية، وتزويدهم بالمعرفة والمهارات اللازمة لاتخاذ التدابير الوقائية المناسبة لحماية البيانات والأنظمة. تشمل هذه العملية تعليم المستخدمين التعرف على أساليب الهجوم الإلكتروني المختلفة مثل البرمجيات الخبيثة والتصيد الاحتيالي، وتعزيز السلوكيات الآمنة كالحرص على استخدام كلمات مرور قوية وتفعيل المصادقة متعددة العوامل، وتعتبر برامج التوعية السيبرانية أحد الركائز الأساسية في تقليل المخاطر الناجمة عن العنصر البشري، وبناء ثقافة أمنية قائمة على الوعي والسلوكيات السليمة. (3)

أهداف التوعية بالأمن السيبراني

تُعدّ التوعية بالأمن السيبراني عنصراً أساسياً في حماية الأفراد والمؤسسات من التهديدات الرقمية، إذ تركز على بناء المعرفة وتعزيز السلوكيات الآمنة في التعامل مع التقنيات. ويمكن تلخيص أهدافها الرئيسة فيما يلي:

1. نشر الوعي والمعرفة الأمنية :تمكين الأفراد من فهم كيفية حماية المعلومات والبيانات الحساسة أثناء استخدامهم للتقنيات الرقمية.
2. تصحيح المفاهيم الخاطئة :مواجهة الاعتقادات غير الصحيحة، مثل الثقة في الروابط أو الرسائل غير الموثوقة، مما يقلل من احتمالية الوقوع ضحية لأساليب الاحتيال السيبراني.
3. تغيير السلوكيات :تشجيع الأفراد على تبني ممارسات أكثر أماناً مثل استخدام كلمات مرور قوية، وتجنب مشاركة المعلومات عبر قنوات غير آمنة.
4. تعزيز الفهم بالتهديدات :رفع وعي المستخدمين بالمخاطر الشائعة مثل البرمجيات الخبيثة ومحاولات الاختراق، بما يضمن استعدادهم لمواجهتها.
5. بناء ثقافة أمنية مؤسسية :غرس الشعور بالمسؤولية المشتركة لدى الموظفين تجاه حماية المعلومات، وعدم حصرها في أقسام تقنية المعلومات فقط.
6. الامتثال للمعايير والتشريعات :مساعدة الأفراد والمؤسسات على الالتزام بالقوانين المحلية والدولية المتعلقة بحماية البيانات.
7. تقليل الخسائر الناتجة عن الأخطاء البشرية :تجنب السلوكيات غير الواعية مثل فتح مرفقات مجهولة المصدر، والتي قد تسبب خسائر مالية أو معنوية.
8. مواكبة التطورات السيبرانية :تزويد الأفراد بالمعرفة المستمرة لمواجهة تطور أساليب الهجمات الإلكترونية.
9. تعزيز المسؤولية الفردية والمؤسسية :ترسيخ القناعة بأن الأمن السيبراني مسؤولية جماعية تتطلب وعياً مستمراً من جميع الأطراف. (4)

من خلال هذه الأهداف يتضح أن التوعية السيبرانية ليست مجرد نشاط تدريبي، بل هي عملية مستمرة تستهدف عقل الفرد وسلوكه وممارساته اليومية، وتوجه الأفراد والمؤسسات نحو الاستخدام الرشيد والمسؤول للتقنية. فهي تمثل البنية الأساسية لأي منظومة أمنية ناجحة، كما يظهر بوضوح مدى ارتباط السلوكيات البشرية بالتوعية السيبرانية.. هذا التركيز على البعد الإنساني يمهّد للانتقال إلى المفهوم الحديث المتمثل في إدارة المخاطر البشرية، والذي ينظر إلى الإنسان باعتباره محور القوة والضعف في آن واحد ضمن المنظومة السيبرانية.

متطلبات التوعية السيبرانية في المؤسسات

- اعتماد وتطبيق برنامج توعية سنوي متعدد القنوات لتعزيز الوعي الأمني وتشكيل ثقافة إيجابية للأمن السيبراني.
- تضمين البرنامج بجميع الموظفين وضمن برامج تهيئة الموظفين الجدد.
- تغطية مواضيع تشمل حماية الأنظمة والبيانات، منع واكتشاف حوادث الأمن، التعامل الآمن مع البريد الإلكتروني والإنترنت، وكذلك ضوابط الوصول والسياسات المتعلقة بالاستخدام المقبول والوصول عن بعد.
- تدريب متخصص للموظفين ذوي المهام السيبرانية الحساسة، مثل العاملين في تطوير البرمجيات والتشغيل الفني للأصول المعلوماتية.
- مراجعة وتقييم البرنامج بشكل دوري باستخدام مؤشرات أداء رئيسية لضمان التحسين المستمر.
- الامتثال للسياسات الوطنية لأمن وسلامة المعلومات خصوصاً سياسة التوعية والتدريب.

سياسة التوعية والتدريب الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات

التوعية بأمن المعلومات تساعد بشكل كبير في حماية البيانات الشخصية والملكية الفكرية والمالية والمعلومات الحساسة والسرية والأنظمة الشبكية والتطبيقات التي تستخدمها **المؤسسة**، وذلك عبر تقديم مفاهيم عامة حول المخاطر والتهديدات وأفضل الممارسات في مجال أمن المعلومات.

على الرغم من اعتبار الانسان في معظم الأوقات الحلقة الأضعف في الدفاعات الإلكترونية للمؤسسة، الا أنه قد يكون في الواقع أقوى درع يمكن لها الاستفادة منه ضد الهجمات الإلكترونية من خلال التوعية والتدريب المناسبين، حيث يمكن تحويل القوى العاملة إلى أفضل خط دفاع ضد مجرمي الفضاء السيبراني.

وفي حين أن "**التوعية**" تشير إلى فهم أساسيات مجموعة من الموضوعات المتعلقة بأمن المعلومات، يولي "**التدريب**" اهتمامًا مفصلاً ومحدداً بتلك الموضوعات، حيث يُمكِّن التدريب على أمن المعلومات الأفراد من اتخاذ قرارات أفضل، ليس فقط في كيفية التعرف على الهجمات الإلكترونية المحتملة والاستجابة لها، ولكن أيضًا للتأكد من أنهم لا يعرضون البيانات عن غير قصد للخطر في عملهم اليومي. توفر التوعية المستوى الأساسي للمعرفة والفهم المناسب للتدريب للبناء عليه، لذا فإن الوعي والتدريب بأمن وسلامة المعلومات نهجان مكملان لبعضهما.

تحدد هذه السياسة الشكل العام لبرنامج للتوعية والتدريب بأمن المعلومات الهادف لتثقيف وتحفيز جميع العاملين بـ**(جهة العمل)** فيما يتعلق بمخاطر المعلومات والأمن والخصوصية والالتزامات ذات الصلة.

1. الغرض

الغرض من هذه السياسة هو رفع مستوى الوعي بأمن وسلامة المعلومات وتحديد مسؤوليات العاملين فيما يتعلق بمتطلبات أمن المعلومات والتزاماتهم تجاهها.

2. النطاق

تنطبق هذه السياسة على جميع الموظفين والموظفين المؤقتين بالإضافة لجميع الأشخاص المرتبطين بـ **(جهة العمل)**، والذين لديهم إمكانية الوصول إلى معلوماتها وأجهزة الكمبيوتر والأنظمة التي يتم تشغيلها أو صيانتها نيابة عنها.

3. السياسة

3.1التوعية بأمن المعلومات

3.1.1 يجب إبلاغ جميع الموظفين بالمواضيع الشائعة لأمن المعلومات وذات الصلة بالعمل، وتحفيزهم على الالتزام بأداء واجباتهم المتعلقة بأمن المعلومات حيالها.

3.1.2 يجب على إدارة /قسم أمن المعلومات [أو قسم مكافئ له] تنظيم أربع ورش عمل (على الأقل) في السنة، ويُلزم كل موظف بالحضور ويتم إبلاغ رئيسه بذلك.

3.1.3 يجب على جميع الموظفين الذين يتمتعون بإمكانية الوصول إلى موارد المعلومات لـ **(جهة العمل)** إكمال البرنامج التدريبي الخاص بأمن المعلومات خلال 30 يوم من تاريخ التوظيف. ويجب إكمال التدريب المستمر لأمن المعلومات بشكل سنوي.

3.1.4 يجب على إدارة /قسم أمن المعلومات استخدام الكتيبات والملصقات وشاشات التوقف وغيرها من الوسائل، للمساعدة في زيادة الوعي بأمن المعلومات في **(جهة العمل)**.

3.1.5 يجب تقديم كتيب خاص بالتوعية الأمنية لكل موظف والصفحة الأخيرة على أن تكون موقعة من قبله.

3.1.6 يجب الأخذ في الاعتبار المعرفة بالسياسات الأمنية أثناء تقييم الموظف.

3.1.7 يجب دمج السياسات والإجراءات في ممارسات **(جهة العمل)** للحفاظ على مستوى عالٍ من التوعية الأمنية الذي يتطلب تدريبًا منتظمًا لجميع الموظفين والمتعاقدين مع **(جهة العمل)**.

3.1.8 يجب إجراء برامج التوعية الأمنية بصفة مستمرة لضمان أن لا تكون التوعية والتدريب كنشاط سنوي فحسب، بل يتم استخدامها للحفاظ على مستوى عالٍ من الوعي الأمني على أساس يومي.

3.1.9 يجب على إدارة /قسم أمن المعلومات تشكيل فريق التوعية الأمنية، بحيث يكون هذا الفريق مسؤول عن تقديم وتطوير برنامج التوعية الأمنية. يوصى بتكوين الفريق من موظفين من إدارات وأقسام مختلفة من **(جهة العمل)** وبمسؤوليات مختلفة تمثل قطاعًا عرضيًا لـ **(جهة العمل)**.

3.1.10 يجب على إدارة /قسم أمن المعلومات تحديد الأدوار في برنامج التوعية الأمنية، بحيث يوفر هذا البرنامج القائم على الوظيفة لـ **(جهة العمل)** مرجعًا لتدريب الموظفين على المستويات المناسبة بناءً

على وظائفهم. يمكن توسيع نطاق التدريب – أو تجميع أو إزالة الموضوعات - وفقًا لمستويات المسؤولية والأدوار المحددة في **(جهة العمل)**.

3.1.11 يجب على فريق التوعية تحديد المقاييس لتقييم التوعية والتدريب: حيث تعد أداة فعالة لقياس نجاح برنامج التوعية الأمنية، ويمكنها أيضًا توفير معلومات قيمة للحفاظ عليه محدثًا وفعالًا، وستختلف المقاييس المحددة المستخدمة لقياس نجاح برنامج التوعية الأمنية لكل مؤسسة بناءً على اعتبارات مثل الحجم والمجال ونوع التدريب.

3.1.12 يجب أن يكون لدى فريق التوعية قائمة مرجعية لبرنامج التوعية الأمنية لتساعد **(جهة العمل)** على تخطيط وإدارة برنامجها التدريبي يمكن استخدام قائمة التحقق الخاصة بالهيئة للمساعدة في التدريب على الوعي الأمني.

3.2التدريب حول أمن المعلومات

3.2.1 يجب أن تحدد إدارة /قسم أمن المعلومات عناصر برنامج تدريبي للتوعية بأمن المعلومات. ويضمن الآليات المناسبة لتنفيذه.

3.2.2 يجب أن يُطلب تدريب إضافي على برامج التوعية بناءً على مهام الموظفين الذين تتطلب مسؤولياتهم صلاحية وإمكانيات الوصول للمعلومات السرية على النحو المحدد في سياسة تصنيف البيانات الخاص بـ **(جهة العمل)**، ويجب إكمال التدريب بشكل سنوي أو دوري.

3.2.3 يجب أن يتضمن برنامج التدريب تدريبًا عاماً إلزاميًا سنويًا، واستطلاعات مجدولة دورياً، وتقييمات التوعية الدورية غير مجدولة لضمان الامتثال للتدريب، واستطلاعات الرأي لتحسين برنامج التدريب والتثقيف التوعوي.

3.2.4 يجب حفظ شهادات إتمام التدريب ونتائجها في ملف الموظف بالموارد البشرية. (5)

المحور الثاني: المخاطر البشرية في الأمن السيبراني

مفهوم المخاطر البشرية

إدارة المخاطر البشرية (HUMAN RISK MANAGEMENT-HRM)

تُعد إدارة المخاطر البشرية نهجاً متقدماً يتجاوز حدود التوعية الأمنية التقليدية. لا تقتصر أهميتها على تحسين تقييم المخاطر وزيادة فاعلية التدريب، بل تتجاوز ذلك إلى إعادة صياغة الطريقة التي تتعامل بها المؤسسات مع الأمن السيبراني من منظور يركز على العنصر البشري.. من خلال إزالة الحواجز التقليدية بين الجوانب التقنية للأمن السيبراني وبرامج التوعية، تفتح إدارة المخاطر البشرية المجال أمام منظومة أمنية أكثر ترابطاً واستجابة وفعالية.

مفهومها

يمكن تعريف إدارة المخاطر البشرية (HRM) " بأنها منهج شامل يركز على تحديد وتقييم وإدارة المخاطر المرتبطة بالسلوك البشري بشكل مستمر، مع العمل على تقليلها بشكل فعّال. هذا المنهج يهدف إلى تحقيق نتائج ملموسة من خلال التركيز على المحفزات السلوكية، لتعزيز ثقافة أمنية تجعل سلوكيات الاستخدام الآمن أمراً طبيعياً وغريزياً داخل بيئة العمل".(6)

أهمية تطوير مفهوم التوعية السيبرانية إلى مفهوم إدارة المخاطر البشرية

الهدف من تطوير مفهوم التوعية إلى مفهوم إدارة المخاطر البشرية في الأمن السيبراني هو تحويل النهج من مجرد نقل المعلومات والتدريب إلى إطار أكثر شمولية ومنهجية يُركّز على تقييم السلوكيات البشرية التي تُشكل نقاط ضعف محتملة داخل المؤسسة، وتحديد أولويات التدخل لمعالجة المخاطر المرتبطة بها.

يهدف هذا التحول إلى:

- الاعتماد على نهج يركز على المخاطر بدلاً من التركيز فقط على التدريب النظري.
- إعادة صياغة التوعية الأمنية بما يتماشى مع أولويات العمل الفعلية للمؤسسة.
- معالجة المقاومة الداخلية للتغيير عبر إشراك الأفراد في فهم أهميتهم في تحسين الأمن السيبراني.
- قياس التأثير باستخدام مؤشرات متوافقة مع مستوى المخاطر التي تواجه المؤسسة.
- تعزيز التأثير وزيادة دعم القيادة لاستراتيجيات تقليل المخاطر البشرية.

بذلك يصبح الأمن السيبراني جزءًا من إدارة المخاطر المتكاملة في المؤسسة، حيث لا يُنظر إليه كخيار تقني فحسب، بل كعملية تشمل تقييم وتحليل وتخفيف مخاطر السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية. وهذا النهج يعزز قدرة المؤسسات على حماية أصولها الرقمية بفعالية أكبر من خلال بناء ثقافة أمنية واعية ومسؤولة بين جميع الأفراد داخل المنظمة.

أهداف التطور إلى إدارة المخاطر البشرية في الأمن السيبرانية

بالتالي، إدارة المخاطر البشرية في الأمن السيبراني تمثل خطوة استراتيجية تغير طريقة التفكير من التعامل مع التوعية كمهمة تدريبية إلى إدارة متكاملة للمخاطر التي تتضمن سلوك الأفراد كعامل رئيسي في نجاح أو فشل الأمن السيبراني. الهدف من تطوير مفهوم التوعية إلى مفهوم إدارة المخاطر البشرية في الأمن السيبراني هو الانتقال من مجرد تقديم التدريب إلى تبني نهج شامل يركز على تحديد، تقييم، وتقليل المخاطر المرتبطة بالسلوكيات البشرية التي قد تهدد أمن المعلومات. هذا التطور يهدف إلى:

- التركيز على المخاطر الأمنية الفعلية بدلاً من التركيز فقط على التدريب النظري.
- ربط التوعية بأولويات العمل لزيادة فعاليتها وتأثيرها.
- التغلب على مقاومة التغيير من خلال إشراك الجميع بفهم أهمية دورهم في الأمن السيبراني.
- قياس التأثير بناءً على مؤشرات تعكس المخاطر الحقيقية التي تواجه المؤسسة.
- زيادة الدعم والموافقة من القيادة لتعزيز جهود إدارة المخاطر.

في الواقع الليبي، يتعامل المسؤولون والموظفون في المؤسسات مع التوعية السيبرانية بتفاوت ملحوظ تبعاً لمدى نضج المؤسسة في مجال الأمن السيبراني و قدرتها على الإيفاء بمتطلباته المحلية والدولية ، وعلى الرغم من الجهود المبذولة لتعزيز الوعي الأمني من خلال ورش العمل والدورات التدريبية التي تنظمها جهات مختلفة مثل الهيئة الوطنية لأمن وسلامة المعلومات و إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية ، و بعض منظمات المجتمع المدني، إلا أن برامج التوعية غالبًا ما يُنظر إليها كمهام ثانوية

أو التزامات شكلية في بعض المؤسسات، حيث تفتقر إلى الدعم والتركيز الاستراتيجي الذي يعكس أهميتها الحقيقية.

يرى بعض المسؤولين الموظفين التوعية السيبرانية كجزء من التدريب الروتيني أو كمتطلب للامتثال، وليس كجزء أساسي من حماية المؤسسة، مما يؤدي إلى مقاومة أو تجاهل بعض السلوكيات غير الآمنة. ومع ذلك، بدأت أعداد متزايدة من المؤسسات تدرك الحاجة إلى ربط التوعية بأهداف العمل الحقيقية وتحويلها إلى برامج مدروسة تقيس تأثيرها بناءً على تقليل المخاطر وتحسين مستويات الأمان الفعلية.

كما أن هناك جهود واضحة لتعزيز الوعي الأمني والثقافة الأمنية بين الموظفين من خلال زيادة مشاركة القيادات وتشجيع الاستثمار في تدريب مستمر ومواكب، إلا أن هذه الجهود تحتاج إلى الاستمرارية والتطوير لتجاوز النظرة التقليدية إلى التوعية كمسألة شكلية والانتقال إلى مفهوم إدارة المخاطر الأمنية القائمة على السلوكيات البشرية، مما يجعل المؤسسات الليبية أكثر قدرة على مواجهة تحديات الأمن السيبراني بفعالية.

بالتالي، فإن التحدي الأكبر أمام المؤسسات الليبية هو تحويل التوعية السيبرانية من مهمة روتينية إلى استراتيجية شاملة مدعومة بقيادة قوية وثقافة مؤسسية فاعلة تقود إلى تقليل المخاطر وتحقيق حماية حقيقية للبنية الرقمية الوطنية.

أنواع المخاطر البشرية في الأمن السيبراني

بناءً على وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) والمعهد الوطني للمعايير والتكنولوجيا بالولايات المتحدة(NIST) ، فإن أنواع المخاطر البشرية الأكثر شيوعًا في الأمن السيبراني تشمل:

1. **الأخطاء البشرية:(Human Error)**

تعتبر الأخطاء البشرية السبب الرئيسي لحوالي 68% من اختراقات البيانات كما أظهرت تقارير، وتشمل ذلك فتح روابط مشبوهة، عدم تحديث الأنظمة، استخدام كلمات مرور ضعيفة، وعدم اتباع الإجراءات الأمنية الصحيحة.

2. **الهندسة الاجتماعية:(Social Engineering)**

خداع الموظفين أو المستخدمين للكشف عن معلومات سرية أو تنفيذ أوامر قد تؤدي إلى اختراق الأنظمة، مثل هجمات التصيد الاحتيالي.(Phishing)

3. **التهديدات الداخلية:(Insider Threats)**

أفعال ضارة أو غير مقصودة من موظفين أو أفراد داخل المنظمة يمكن أن تؤدي إلى تسرب المعلومات أو تعطيل الأنظمة.

4. **نقص الوعي الأمني والتدريب:(Lack of Security Awareness and Training)**

قلة التوعية لدى العاملين تؤدي إلى ضعف القدرة على التعرف على التهديدات والتعامل معها بشكل صحيح،

5. **سوء إدارة صلاحيات الوصول:(Poor Access Management)**

منح صلاحيات زائدة أو غير دقيقة للعاملين يسمح لهم بالوصول غير المصرح به إلى بيانات أو أنظمة حساسة، مما يزيد من المخاطر.

6. **الإهمال في صيانة الأنظمة:(Neglecting System Maintenance)**

عدم تحديث وتصحيح الأنظمة والبرمجيات يفتح ثغرات يستغلها المخترقون، وهو جزء من الأخطاء البشرية المشتملة على ضعف الوعي والتدريب. (4)

المحور الثالث: التطور المفاهيمي من التوعية إلى إدارة المخاطر البشرية.

ما وراء التوعية السيبرانية:

في كثير من الحالات، تكشف بعض الحوادث في الشركات عن فجوة حقيقية بين برامج التوعية الأمنية والواقع الفعلي للمخاطر البشرية. فعلى سبيل المثال، تعرضت إحدى الشركات مؤخراً لاختبار اختراق شمل حملة واسعة للهندسة الاجتماعية والتصيد الإلكتروني. ورغم أن الشركة كانت تعتمد على أحد أشهر برامج تدريب التوعية الأمنية، جاءت نتائج الحملة مفاجئة للغاية؛ حيث سقط العديد من الموظفين المستهدفين في الفخ بسهولة.

عند مراجعة التفاصيل، تبين أن الأفراد الذين تم اصطيادهم خلال الحملة كانوا قد حصلوا على تقييمات مرتفعة جداً في اختبارات التدريب والمحاكاة الدورية. ولإكمال الصورة، تم تحليل بيانات نظام إدارة معلومات وأحداث الأمان (SIEM) وسجلات أمن نقاط النهاية، فظهر نمط سلوكي مقلق: معظم الخروقات الأمنية الحقيقية التي حدثت خلال الفترة السابقة ارتبطت بثلاثة موظفين فقط – أحد كبار المدراء التنفيذيين، ومسؤول موارد بشرية، ومدير تقنية معلومات. والمثير للاهتمام أن هؤلاء الأشخاص أنفسهم كانوا مصنفين ضمن الفئة "الأقل خطورة" بحسب نتائج التدريب التقليدي.

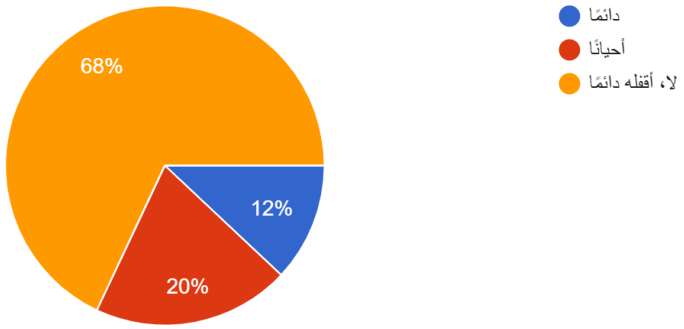
تُظهر هذه الحالة أن مجرد اجتياز الاختبارات لا يعني بالضرورة أن الموظف يتمتع بسلوك آمن في بيئة العمل الفعلية، مما يبرز أهمية التركيز على إدارة المخاطر البشرية الحقيقية وليس الاكتفاء بالتدريب النظري فقط.

فيما مثال عن أهمية تحليل السلوك البشري قبل تقديم التوعية باستخدام استبيان موجه للموظفين من قبل قسم التوعية والعلاقات بالهيئة الوطنية لأمن وسلامة المعلومات لإحدى الشركات المحلية الليبية نجد أن سلوكاً قد يعتبره البعض عادياً يراه المتخصص في مجال الأمن السيبراني ثغرة قد ينتج عنها تهديد محتمل.. (6)

السؤال:

هل تترك جهازك مفتوحًا عند الابتعاد عنه في المكتب؟

50 ردًا



ترك الجهاز دون قفل عند الابتعاد عنه داخل مؤسسة تقدم خدمات تقنية وتتعامل مع بيانات حساسة لعملائها يُعتبر سلوك غير آمن ويُصنّف كخطر سيبراني مباشر..

الخطر الناتج عن سلوك بشري خاطئ	الوزن (1-5)	الأثر المحتمل
الوصول غير المصرح به إلى بيانات حساسة أو سرية	5	انتهاك سرية البيانات، فقدان الثقة
تنفيذ أوامر ضارة (تثبيت برامج خبيثة، حذف بيانات، تعديل إعدادات)	5	تعطيل الأنظمة، اختراق كامل للجهاز
سرقة حسابات المستخدم (جلسات مفتوحة على البريد أو الأنظمة)	4	اختراق الحسابات واستخدامها بشكل غير شرعي
تسريب بيانات العملاء أو معلومات المشاريع الجارية	4	تضرر سمعة المؤسسة، خسارة عملاء
استخدام الجهاز لعمليات غير قانونية باسم المؤسسة	5	مسؤولية قانونية، تشويه سمعة المؤسسة

قد لا يعي الموظف بهذه الشركة أن سلوكاً بسيطاً يستمر لدقائق معدودة يمكن أن يكون له أثر خطير ومحتمل.. وهنا تأتي المرحلة التالية وهي إدارة هذا السلوك عبر اتباع سلسلة من الخطوات المنهجية.

ومنها يظهر أن الجانب البشري هو أحد أهم عوامل فشل أو نجاح تطبيق خطط الأمن السيبراني في المؤسسة، لذا تقدم التوصيات بشكل دائم على تركيز الجهود على التوعية المقترنة بالتدخل المطلوب لتعديل السلوك، والتدريب المستمر، ومشاركة القادة في تعزيز بشكل استراتيجي ثقافة الأمن السيبراني داخل المؤسسات.

مراحل إدارة المخاطر البشرية في مجال الأمن السيبراني

كما تم ذكره سابقاً خطوات منهجية مخصصة تعكس الخصوصيات الأمنية والتقنية لهذا المجال من أجل حماية أنظمة المعلومات والأصول الرقمية من التهديدات المرتبطة بالعامل البشري. هذه المراحل تشمل:

1. تحديد الأصول والثغرات البشرية: يشمل جرد الأصول الرقمية والأنظمة والموظفين مع التركيز على نقاط الضعف البشرية مثل قلة الوعي الأمني، الأخطاء البشرية، والتصرفات غير الآمنة.
2. تحليل وتقييم المخاطر البشرية: دراسة التهديدات التي قد تأتي من الخطأ البشري، مثل التصيد الاحتيالي، استخدام كلمات مرور ضعيفة، أو السلوك غير المسؤول، وتقييم احتمالية حدوثها وتأثيرها على الأمان.
3. وضع استراتيجيات الادارة والتخفيف: تطوير سياسات واضحة للأمن السيبراني تشمل تعليم وتدريب الموظفين على الممارسات الآمنة، إنشاء ضوابط فنية مثل التوثيق متعدد العوامل، وتطبيق إجراءات مثل مراقبة الأنشطة المشبوهة.
4. التنفيذ والمراقبة المستمرة: تطبيق الإجراءات الأمنية والمراقبة الدائمة لسلوك الموظفين والتحقق من الالتزام بالسياسات، إلى جانب تحديث التدريبات والتقنيات استجابةً للمخاطر الجديدة.
5. الاستجابة للحوادث والتعافي: وضع خطط استجابة فعالة للحوادث الناتجة عن أخطاء بشرية أو اختراقات، تتضمن التحقيق، التخفيف، والتعافي لضمان استمرارية العمل وحماية البيانات.
6. التوعية والتدريب المستمر: رفع وعي الموظفين بشكل دوري حول أهمية الأمن السيبراني والمخاطر الإنسانية، مع تنظيم برامج تدريبية وتحديثات دورية لتعزيز الممارسات الأمنية.

هذه المراحل تشكل دورة مستمرة ومتكررة تهدف لتقليل المخاطر البشرية التي تعتبر الحلقة الأضعف في منظومة الأمن السيبراني، وتعزز من حماية المؤسسة ضد التهديدات المتطورة

المراجع:

1. European Union Agency for Cybersecurity (ENISA). (2016). *Definition of Cybersecurity: Gaps and overlaps in standardization*. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity.

2. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). "Cyber security awareness campaigns: Why do they fail to change behavior? "

3. SANS Institute. (2018). *SANS security awareness report 2018*. Retrieved August 20, 2025, from https://securitydelta.nl/media/com_hsd/report/201/document/2018-SANS-Security-

4. ENISA "Cybersecurity Threats for 2030 – Update 2024" "Cybersecurity – the Human Factor".
https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report

5. دليل السياسات الوطنية لأمن وسلامة المعلومات، فريق إعداد السياسات الوطنية لأمن وسلامة المعلومات، الهيئة الوطنية لأمن وسلامة المعلومات، نوفمبر 2021.
https://2h.ae/RAUG

6. استبيان تقييم مخصص لشركة محلية أغسطس 2025، قسم التوعية والعلاقات، إدارة معالجة حوادث المعلوماتية والشبكات، الهيئة الوطنية لأمن وسلامة المعلومات
https://forms.gle/ZyuY8zqTxDTHrvtv8

دليل أنير للتحقق من المحتوى الرقمي

الفهرس

3. التحقق من المحتوى المرئي

3.1 التحقق من الصور

3.1.1 البحث العكسي عن الصور
3.1.1.1 محرك بحث جوجل "Google Image Search"
3.1.1.2 أداة "Tineye"
3.1.1.3 محرك بحث "Yandex Images"
3.1.1.4 محرك بحث "Bing"

3.1.2 التحقق من التلاعب في الصور
3.1.2.1 أداة "Forensically"

3.2 التحقق من مقاطع الفيديو
3.2.1 البحث عن مقاطع الفيديو باستخدام الكلمات المفتاحية
3.2.2 البحث عن الفيديو باستخدام موقع يوتيوب "Youtube"
3.2.3 البحث باستخدام صورة من فيديو

4. اثنان في واحد: أداة "InVid" للتحقق

5. بيانات الموقع الجغرافي
5.1 "Google Maps"
5.2 "Google Earth"
5.3 "NASA Earth Observatory"
5.4 "Wikimapia"
5.5 "Google Translate"

6. بيانات مواقع الويب

6.1 امتداد الدومين "Domain Extension"
6.2 أداة "ScamAdviser"
6.3 أدوات أخرى

7. التحقق من حسابات وسائل التواصل الاجتماعي **"Social Media"**

7.1. الحسابات الموثقة على فيسبوك وانستاجرام

7.2. الحسابات الموثقة على تويتر **"X"**

7.2.1. علامة التوثيق الزرقاء

7.2.2. علامة التوثيق الرمادية

7.2.3. علامة التوثيق الذهبية

7.3. صفحات رسمية غير موثقة

7.3.1. البحث عن الموقع الرسمي عبر محركات البحث

7.3.2. تحليل بيانات الموقع

7.3.3. زيارة الموقع

7.3.4. معايير شفافية الفيسبوك

7.4. **"LinkedIn"**

7.5. **"WebMii"**

8. خدمات أرشفة المواقع

8.1. أداة العودة بالزمن **"Wayback Machine"**

8.1.1. طريقة البحث عن نسخ مؤرشفة سابقاً

8.1.2. طريقة أرشفة منشور أو تغريدة للعودة لها لاحقا أو لاستخدامها كمرجع

- الخاتمة
- إخلاء طرف
- عن أنير
- سياسة استخدام دليل أنير للتحقق من المحتوى الرقمي
- الهوامش

المقدمة

في عصر اليوم، لا يمكن لأي شخص باختلاف عمره، أو جنسه، أو خلفيته الثقافية، أن ينكر التأثير الواسع والعميق الذي تمتلكه وسائل التواصل الاجتماعي على حياتنا اليومية. إن الكثير من آرائنا وقراراتنا ورؤيتنا للحياة وكيفية التعامل معها هي نتيجة ما نطالعه يومياً على هذه الوسائل. وقد عاصر كل منا على الأقل حدثًا عالميًا واحدًا، كان لوسائل التواصل الاجتماعي فيه دور مهم، فقد بنيت عليها ثورات، وانتشرت أيديولوجيات، وتغيرت سياسات.

في خضم هذا التدفق المستمر من المحتوى الرقمي، ينبغي على مستخدمي/ات هذه المنصات أن يعوا جيدًا الاحتمالية العالية لأن يكون بعض هذا المحتوى غير دقيق أو غير حقيقي. يمكن ببساطة تشبيه رحلتك اليومية خلال حساباتك على هذه المنصات، بنزهة في حقل ألغام، إن لم تكن حذرًا من خلال التحقق من مصداقية كل ما تقرأه أو تتلقاه، قد تكون العواقب جسيمة.

لهذا الهدف تم إعداد دليل أنير للتحقق من المحتوى الرقمي، ليكون مصدرًا مرجعيًا للتعرف على أنواع المحتوى والمنشورات المتداولة عبر وسائل التواصل الاجتماعي، وكيفية التحقق من مصداقيتها باستخدام العديد من أدوات وآليات التحقق، بالإضافة إلى العديد من الأمثلة التي من شأنها أن تساعدك على فهم وتحليل أنواع المحتوى على الإنترنت، بهدف التحقق من الأخبار ومكافحة اضطراب المعلومات.

ينقسم هذا الدليل الى محورين رئيسيين، يتطرق الأول إلى ماهية اضطراب المعلومات وتأثيراته المجتمعية ودور تدقيق المعلومات، ويتناول المحور الثاني الأدوات التقنية مفتوحة المصدر، وكيفية استخدامها في التحقق من المحتوى في الفضاء الرقمي.

(I) المحور الأول: مكافحة اضطراب المعلومات

1. اضطراب المعلومات

يوصف اضطراب المعلومات بأنه التأثير الناشئ من تداول ثلاثة أنماط رئيسية للمعلومات على شبكات التواصل الاجتماعي ومواقع الإنترنت. تؤثر هذه المعلومات بشكل سلبي على المجتمع، وتجتمع معاً لتكوين اضطراب يهدد السلامة العامة للأفراد، وفي العادة يزيد هذا التأثير في أوقات الأزمات والحروب والصراعات والتوتر السياسي.

الأنماط الرئيسية الثلاثة لاضطراب المعلومات: [1]

اختلف المجتمع الأكاديمي على تعريف الأقسام الرئيسية لاضطراب المعلومات، حيث توجد العديد من التقسيمات لأنواع المعلومات التي تصنع تأثير اضطراب المعلومات. ولكن حسب منظمة الأمم المتحدة للتربية والعلم والثقافة "اليونسكو" يمكن تقسيم هذه الأنماط إلى ثلاثة أنواع رئيسية:

1.1. **المعلومات الخاطئة (Misinformation):**

هي المعلومات الخاطئة الي يتم نشرها بدون عمد، والسبب أحياناً يعود لقلة وعي المستخدمين/ات أو السرعة في نشر الأخبار.

1.2. المعلومات المضللة (Disinformation): [2] [3]

هي معلومات خاطئة يتم نشرها بشكل متعمد، وأحياناً بأنماط ممنهجة بهدف الترويج لفكرة وتهميش أخرى، تنشط في العادة في أوقات الصراعات السياسية والانتخابات، وتهدف للتأثير على الرأي العام وتوجيهه.

(أثناء فترة الانتخابات الأمريكية، روجت حملة تضليل ممنهجة بأن المرشحة لنائب الرئيس كاميليا هاريس ليست من أصول سوداء، وذلك كوسيلة لتقليل الأصوات المؤيدة لها، بينما هي في الواقع تعتبر أمريكية سوداء لأم هندية وأب جمايكي.)

1.3. المعلومات الضارة (Malinformation):

هي معلومات صحيحة ويتم نشرها بشكل متعمد، ولكن بهدف تشويه سمعة، أو إلحاق الضرر النفسي، أو الجسدي بشخص، أو مؤسسة، أو دولة معينة، ومن أمثلة المعلومات الضارة خطاب الكراهية والتشهير وبعض أشكال التسريبات.

(مثال واضح على استغلال المعلومات الضارة يتجلى عندما تم تسريب رسائل البريد الإلكتروني الخاصة بإيمانويل ماكرون قبل الانتخابات التمهيدية في السابع من مايو. هذه الرسائل الإلكترونية كانت حقيقية، ومع ذلك، تم تسريبها إلى الجمهور قبل ساعات قليلة من فرض حظر قانوني على أي تغطية انتخابية قبل بدء عملية التصويت. هذا التسريب كان هدفه تحقيق أقصى قدر من الضرر لحملة ماكرون.)

اضطراب المعلومات والمجتمع [4]

لاضطراب المعلومات تأثير اجتماعي واسع وخطير يطال جميع الأصعدة في المجتمع، إذ يساهم في المساس بمجالات حيوية مثل الصحة، والاقتصاد، والسياسة. ويشكل تهديداً للأمن والسلامة العامة من خلال نشر الفتن وتأجيج الحروب، وخلق فوضى اجتماعية قد تؤثر على أساسيات الحياة مثل الكهرباء، والوقود، وأسعار السلع، وغيرها.

- لماذا يتم نشر المعلومات الخاطئة والمضللة والضارة؟ [8] [7] [6] [5]

يقف بشر مثلنا خلف نشر أي محتوى موجود على الإنترنت، ولهذا يمكن فهم الكثير حول ظاهرة اضطراب المعلومات ومكافحتها، من خلال فهم الأسباب والدوافع التي تجعل أي شخص ينشر محتوى غير دقيق.

تتعدد دوافع نشر المعلومات الخاطئة والمضللة والضارة، وتختلف حسب الأنماط المختلفة للمعلومات. قد يكون الهدف من نشرها هو الكسب المادي المباشر، أو الرقمي على شبكة الإنترنت، أو التأثير السياسي والاجتماعي، أو لأسباب النزاعات الثقافية والدينية، وغيرها.

- **بعض الأسباب التي تدفع الأفراد أو الجهات إلى نشر معلومات غير دقيقة:**

- **الكسب المادي أو الرقمي:**

تعتبر الرغبة في تحقيق الكسب المادي والرقمي من أهم الدوافع وراء نشر المعلومات غير الدقيقة. تستخدم هذه المعلومات لجذب الأفراد للتفاعل مع رابط أو إعلان معين، والحصول على عدد أكبر من النقرات والمشاهدات وبالتالي الإيرادات الإعلانية. ويستخدم المحتوى المضلل أيضًا للاحتيال على الأشخاص الباحثين عن معلومات محددة أو منتجات غالية الثمن، واستغلالهم، وقد تستخدم الشركات والمؤسسات المحتوى المضلل للترويج لمنتجاتها وزيادة المبيعات.

- **التأثير السياسي والاجتماعي:**

يُعتبر التأثير السياسي والاجتماعي من الدوافع المهمة لنشر المعلومات الخاطئة والمضللة، مثل تشويه سمعة الخصوم السياسيين خلال الحملات الانتخابية. أو للتأثير على آراء الناس وتوجيه الرأي العام نحو آراء معينة أو سياسات محددة.

- **النزاعات الثقافية والدينية:**

قد تنتشر المعلومات المضللة والضارة في سياق النزاعات الثقافية والدينية، بهدف التحريض على الكراهية وتعزيز الانقسامات، ودعم أيديولوجية على حساب أخرى، وجذب أنصار جدد لقضية معينة.

- **الانتقام الشخصي والسياسي:**

يُمكن للأفراد أو الجهات أن ينشروا معلومات ضارة ومضللة بهدف الانتقام من شخص معين أو دولة أو مؤسسة، وذلك لتشويه سمعتهم أو إلحاق الضرر النفسي أو الاقتصادي بهم.

- **الأغراض الإجرامية والاحتيالية:**

قد يُستخدم نشر المعلومات المضللة في عمليات احتيالية وأغراض إجرامية للحصول على معلومات شخصية حساسة أو تحقيق مكاسب غير مشروعة.

- **التضليل صناعة**

في عصر صناعة التضليل، تعد وسائل التواصل الاجتماعي بما تتيحه من سهولة الوصول والانتشار، أداة محورية لنشر الأخبار الخاطئة والمعلومات المضللة، لا سيما مع تطور التكنولوجيا وتقنيات الذكاء الاصطناعي. حيث يمارس التضليل على هذه المنصات بشكل احترافي ومنظم، في صناعة منظمة تستغل مشاعر الناس وتتلاعب بها.

تُقدم هذه الصناعة الاحترافية المعلومات الخاطئة بشكل مغرٍ وجذاب للجمهور، مستهدفةً الجانب العاطفي للأفراد، وتسعى لإثارة الغضب والخوف أو استدراج التعاطف والتأثير على المشاعر. تُعد هذه الاستراتيجيات فعالة في جذب انتباه المستخدمين/ات وتشجيعهم/ن على المشاركة ونشر المعلومات دون التحقق من صحتها.

- **مكافحة اضطراب المعلومات** [9]

بالرغم من أن السياسات العامة والعمل المؤسسي قد يساهم في التقليل من آثار اضطراب المعلومات، إلا أن أكبر وسيلة لمكافحة اضطراب المعلومات، تكون على مستوى الأفراد، فالوعي بأساليب التفكير النقدي والمعرفة بأساليب التحقق من المعلومات هي أفضل سلاح لمواجهة آثار اضطراب المعلومات.

- وبعبارة أبسط، يمكن وضع قاعدة ذهبية كحجر أساس في مواجهة هذا التأثير، وهي:

(عدم تصديق أي معلومة على شبكة الإنترنت عامةً أو مواقع التواصل الاجتماعي خاصةً إلا بعد التأكد من موثوقية المصدر، أو التحقق من المعلومة بشكل شخصي.)

2. نظرة عامة عن تدقيق المعلومات [10] [11]

تدقيق المعلومات أو التحقق من المعلومات "Fact-checking" هو عملية التحقق والتأكد من صحة المعلومات المتداولة عبر وسائل التواصل الاجتماعي والإنترنت، من خلال فحص مصداقية المصادر والتحقق من حقيقة المعلومات المنشورة، وذلك من قبل مؤسسات/مبادرات تدقيق المعلومات ومدققي/ات المعلومات "Fact-checkers" باتباع منهجيات وأدوات محددة لتحليل الادعاءات والوصول إلى نتيجة تسمح بتقييم الأخبار بناءً على صحتها أو عدم صحتها.

يهدف تدقيق المعلومات إلى تزويد الجمهور بمعلومات دقيقة وموثوقة، ومكافحة اضطراب المعلومات. وتعد هذه العملية جزءًا هامًا في بناء الثقة وتعزيز الوعي العام بين الناس حول صحة المعلومات التي يتلقونها ويشاركونها عبر الإنترنت.

2.1. نبذة تاريخية عن تدقيق المعلومات

تاريخيًا، اعتمدت العديد وسائل الإعلام على تدقيق المعلومات قبل نشرها. كان الصحفيون/ات والمحررون/ات يقومون بفحص المعلومات والمصادر والتحقق من صحتها قبل نشرها في الصحف والمجلات والمنصات الإعلامية الأخرى.

ولكن مع ظهور وسائل التواصل الاجتماعي والإنترنت، أصبح من السهل على أي شخص نشر معلومات بسرعة وسهولة دون الحاجة إلى التحقق من صحتها. واحتلت قضية تدقيق المعلومات أهمية بالغة خلال الانتخابات الأمريكية عام 2016 ورواج مصطلح "الأخبار الكاذبة Fake news" في هذه الفترة، اتسع نطاق الأخبار الخاطئة والمضللة التي تأثرت بها الحملات الانتخابية والرأي العام الأمريكي. تم التحقق من صحة الكثير من هذه الأخبار وتبين أنها زائفة، مما أثر بشكل كبير على المشهدين السياسي والاجتماعي في الولايات المتحدة وحول العالم.

من جانب آخر، ومع بداية جائحة كوفيد-19، واجه العالم موجة كبيرة من المعلومات الخاطئة والمضللة حول فيروس كورونا المستجد، وكان من الضروري التحقق من صحة هذه المعلومات قبل اتخاذ أي قرارات أو نشرها. انتشرت الشائعات والمعلومات الخاطئة بسرعة كبيرة عبر وسائل التواصل الاجتماعي وأدت إلى زيادة حالات الذعر والتشويش على الرأي العام.

من هنا، ازدادت الحاجة لمؤسسات ومبادرات تدقيق المعلومات، وذلك للتعامل مع التحديات المعاصرة لانتشار المعلومات الخاطئة والمضللة على نطاق واسع. تستخدم هذه المبادرات التكنولوجيا والأدوات المتطورة لفحص وتحليل المعلومات والتأكد من صحتها.

بلغة أبسط، يعد تدقيق المعلومات وسيلة هامة لتزويد الجمهور بمعلومات دقيقة وموثوقة والحد من اضطراب المعلومات وتعزيز الوعي العام.

2.2. الشك والسؤال [12] [9]

كما ذكرنا سابقاً في فقرة مكافحة اضطراب المعلومات، تظل الخطوة الأولى والأساسية في مكافحة اضطراب المعلومات هي عدم التسليم المطلق بصحة أي معلومة، والتشكيك في حقيقة أي معلومة في الفضاء الرقمي. ولكن للتشكيك بطريقة مدروسة، وللحصول على المعلومات الدقيقة في كل مرة، يجب علينا طرح الأسئلة المناسبة عند تعرضنا للمحتوى على الإنترنت.

2.2.1. ما هو مصدر المعلومة؟

يخبرنا التساؤل حول مصدر المعلومات الكثير حول مصداقيتها. وللتحقق من مصدر الخبر، يجب تذكر النقاط التالية:

- **المصدر الموثوق هو الخيار الأكثر أمانًا.**

في حالة عدم التعرف على المصدر، أو في حالة كان المصدر غير مخول لنشر معلومات متخصصة، يجب أن نتحرى عن حقيقته ثم نتساءل "لماذا يتم نشر هذه المعلومات؟ وما النية وراء ذلك؟".

- **إذا لم يكن هناك مصدر، ابحث/ي عنه.**

إذا لم يكن هناك أي مصدر للمعلومة، يجب أن نبحث عن مصدرها سواء باستخدام طرق البحث عن الصور أو الكلمات المفتاحية أو غيرها.

- **إذا لم تبدُ المعلومة صحيحة، احذر!**

نلاحظ في العديد من المعلومات الخاطئة عدم احترافية صياغتها. حتى لو تم نشرها بطريقة تحاول محاكاة المواقع الموثوقة أو على وسائل التواصل الاجتماعي. يكمن الفرق عادة بين الخبر الصحيح والمزيف في الدلائل الصغيرة مثل: روابط مزيفة، أخطاء إملائية، أو تنسيقات غريبة في وسائل التواصل الاجتماعي.

2.2.2. ما الذي ينقصها؟

يمكن نشر المعلومات المضللة من خلال نشر قصة غير متكاملة، أو أجزاء مقتطعة منها، لهذا يجب عند مطالعة الأخبار أن نتذكر التالي:

- **الحصول على القصة كاملة، ليس فقط العنوان.**

يمكن لنقرة واحدة أن تساعدنا على اكتشاف الأخبار الكاذبة. يجب علينا قراءة القصة بأكملها والانتباه إلى الصور والأرقام والاقتباسات التي لا تحتوي على مصادر أو التي قد تكون نقلت خارج سياقها.

- **غالبًا ما تحتوي الأخبار الكاذبة على صور أو فيديوهات تم تعديلها.**

يمكن استخدام الصور الحقيقية في غير سياقها عن طريق إرفاقها بتواريخ خاطئة أو نص وصفي غير دقيق. ويمكن تعديل الفيديوهات وتغيير الأصوات المصاحبة لها قبل نشرها، لهذا ينبغي دائماً التحقق من دقة الصور والفيديوهات المرافقة للأخبار.

- **الاطلاع على ما يقوله الآخرون.**

من المهم جداً الاطلاع على تصريحات ومقالات مواقع الأخبار الموثوقة أو مدققي/ات المعلومات. خاصة في حالات الطوارئ، إذ يفضل تفقد المواقع أو المصادر الرسمية الخاصة بالسياق المعني قبل نشر وتصديق أي خبر.

2.2.3. كيف تشعر حيالها؟

من العلامات التي تثير الشك حول مصداقية أي خبر، هي اعتماده بشكل كبير على تحفيز رد فعل عاطفي لدى القارئ. للتحقق من مصداقية خبر ما، يمكن للنقاط التالية أن تساعد:

- **يحاول صناع الأخبار الكاذبة التلاعب بمشاعرنا.**

صناع المعلومات الخاطئة والمضللة على علم بأن مشاعر مثل الغضب أو القلق أو الغموض قد تثير عاطفتنا، وبالتالي تزيد من احتمالية الحصول على المزيد من التفاعل والمشاركات والنقرات. لذلك، عند مواجهتنا لمعلومة معينة تثير مشاعرنا يجب علينا التوقف والتفكير في كيفية التحقق منها قبل مشاركتها.

- **إذا بدا الأمر جيدًا لدرجة يصعب تصديقها، فمن المحتمل أن يكون كذلك.**

يمكن استخدام الأمل للتلاعب بنا. في معظم الأحيان، الحلول السحرية لا وجود لها في العالم الحقيقي، تحقق من كل الأخبار التي تعد بحل سريع، كسب سريع، أو شفاء سريع.

- **لا تكن الشخص الذي لا يكتشف النكتة.**

أحيانًا لا تكون النكات والطرق السردية الساخرة على الإنترنت واضحة. يجب علينا الانتباه للتفاصيل المضحكة أو المثيرة للجدل، وطريقة صياغتها. لتحديد السخرية من الزيف، لو لم تكن أكيدًا من جدية الخبر، الأفضل دائما أن تسأل.

3. أمثلة عن أنواع المحتوى المتداول على الإنترنت ومنصات التواصل الاجتماعي:

إن البيئة الأكثر زخماً بإضراب المعلومات هي وسائل التواصل الاجتماعي، فخلال تصفحنا لهذه المواقع، نصادف عدداً كبيراً من المحتوى الشخصي والمحتوى الصادر من كيانات، أو هيئات مدنية، أو حكومية، أو دولية، أو غير ذلك.

3.1. محتوى ساخر:

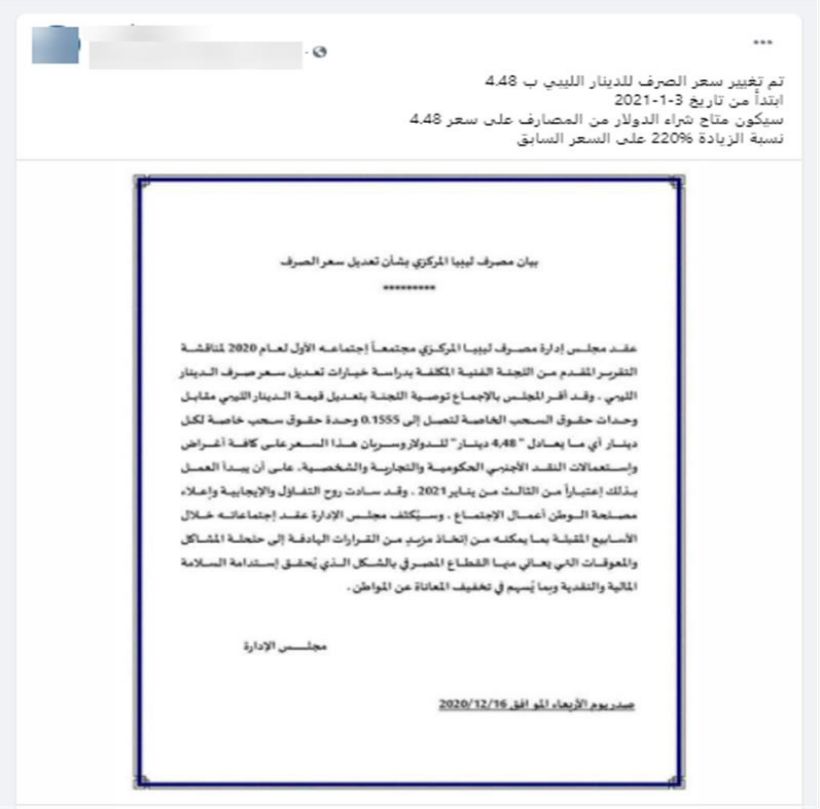
هو محتوى يهدف إلى السخرية، أو الضحك، أو التعليق غير الجاد على أمر أو حدث ما، ولا يعتبر مصدرًا لاستسقاء المعلومات. ويعد هذا النوع من المحتوى أداةً للنقد الحاد بعض الأحيان، ولا يتعدى حد التهكم والسخرية أحياناً أخرى.

(مثال توضيحي لمحتوى ساخر)

3.2. محتوى يتم مشاركته:

يكون هذا المحتوى مأخوذًا من حسابات أخرى، يُشارَك أو يُعاد نشره. الهدف من المشاركة قد يكون من أجل توصيل المحتوى إلى جمهور أوسع، أو التعليق على ما هو مذكور في المحتوى إما تأييدًا أو معارضةً، أو حتى بهدف التهكم.

(مثال عن المحتوى الذي يتم مشاركته من صفحات/حسابات فيسبوك أو على تويتر "X" من خلال زر "المشاركة" أو "إعادة التغريد")



(مثال عن المحتوى الذي يتم مشاركته من صفحات/حسابات فيسبوك أو تويتر "X" من خلال تصوير المنشور ونشره كصورة.)

(مثال عن المحتوى الذي يتم مشاركتها من صفحات/حسابات فيسبوك أو تويتر "X" من خلال نسخ المحتوى ونشره.)

3.3. محتوى إعلاني:

وهو عبارة عن إعلانات تهدف إلى الوصول إلى عدد أكبر من الأشخاص، إما بهدف تجاري (إعلان لمُنتج معيّن مثلاً) أو إعلانات بهدف غير تجاري (الإعلان عن صفحة أو محتوى على الفيسبوك أو الترويج لمنظمة أو مبادرة معينة مثلاً).

(مثال لمحتوى إعلاني تجاري - منشور ممول على فيسبوك)

(مثال لمحتوى إعلاني توعوي - منشور ممول على فيسبوك)

3.4. محتوى رسمي:

وهو محتوى يصدر من جهات حكومية (مثل منشور من وزارة الصحة أو من المصرف المركزي)، أو محتوى يصدر من جهات أممية (من المفوضية السامية للأمم المتحدة لشؤون اللاجئين، أو منظمة الهلال الأحمر، أو الصليب الأحمر الدولي)، أو محتوى يصدر من شركات أو جهات ذات العلاقة بحدث أو منتج معين (مثل منشور من شركة فايزر يتعلق بدواء لعلاج فيروس كوفيد-19).

(مثال لمحتوى رسمي - منشور توضيحي من جهات حكومية)

(مثال لمحتوى رسمي - منشور توضيحي من جهات أممية)

3.5. محتوى يعبر عن مواقف أو آراء شخصية:

هو محتوى يعرض فيه الأشخاص مواقف أو آراء شخصية تعبر عن التوجهات والقناعات، إما "مع" أو "ضد" الموضوع الذي يجري الحديث عنه. هذا النوع من المحتوى عادةً لا يمكن أن يخضع للتدقيق.

(مثال لمحتوى يعبر عن آراء شخصية)

كل هذه الأمثلة عن أنواع المحتوى التي يمكن أن يصادفنا على مواقع التواصل الاجتماعي، هو عبارة عن "معلومات". بعض هذه المعلومات لم ترد بصيغة جدّية أو صيغة خبر. لهذا يجب أن نتذكر أن المعلومات التي نراها ونتفاعل معها هي صنع بشري. وبالتالي لا يجب علينا كجمهور اتخاذ قرارات بناء عليها أو المشاركة في نشرها.

- لكن ما الذي يعطي المعلومات مصداقية للاعتماد عليها؟

الجواب يكمن في أهمية المصادر الموثوقة. عندما نتعامل مع معلومة، يجب أن نتأكد من أنها مدعومة بمصادر موثوقة ومواقع ذات مصداقية.

- فمثلاً:
- إذا كنا نتعامل مع معلومات طبية، يمكننا اللجوء للتأكد منها من خلال منظمات صحية رسمية مثل: منظمة الصحة العالمية.
- وفيما يتعلق بالمعلومات الفلكية، فإن ناسا تُعتبر مصدرًا علمياً موثوقاً.

بالاعتماد على المؤسسات المعتمدة والمتخصصة والعلمية، نستطيع أن نضمن أن المعلومات التي نعتمد عليها هي موثوقة ودقيقة. لكن يجب توخي الحذر في اختيار المصادر، حيث قد تنتشر المعلومات الخاطئة والمضللة أيضًا من خلال مواقع تبدو موثوقة لكنها في الحقيقة غير ذلك!

مجددًا، المبدأ الذي يجب اعتماده دائمًا عند التعامل مع المعلومات، هو عدم تصديق أو نشر أي معلومة إلا إذا كانت مدعومة بمصدر رسمي وموثوق. عندما يكون لدينا شك في صحة معلومة، يجب أن نبحث عن مصادر موثوقة ومؤسسات علمية قبل اتخاذ أي قرار أو مشاركة المعلومة.

4. تدقيق المعلومات كمهنة [10]

مع ازدياد عدد المعلومات الخاطئة والمضللة على الإنترنت، أصبح من الصعب للمستخدمين/ات البسطاء تفريق طبيعة الأخبار لمعرفة ما هو الصحيح أو المضلل أو الزائف بنفسه، ولهذا السبب بادرت العديد من المؤسسات الإعلامية بإنشاء فرق ووحدات خاصة لتدقيق المعلومات، وذلك بتعيين صحفيين/ات ومدققي/ات معلومات للتقصي من صحة العديد من الادعاءات المختلفة؛ لمكافحة الشائعات ونفي الأخبار الخاطئة المنتشرة.

يتجلى دور هذه الفرق في البحث المعمق والتقصي عن حقيقة الأخبار ومشاركة النتائج على الإنترنت ومواقع التواصل الاجتماعي؛ لمكافحة المعلومات المغلوطة. ويعتمد مدققو/ات المعلومات على منهجيات وأدوات عديدة للوصول إلى الحقيقة.

- **تدقيق المعلومات بكفاءة عالية**

4.1. فصل الحياة العملية عن الحياة الشخصية:

تعتبر الموضوعية والحياد وعدم التحزب السياسي من السمات الضرورية التي يجب أن يتحلى بها مدققو/ات المعلومات؛ وذلك لضمان نزاهة وحياد وموضوعية المقال، ولكن مثلما أشرنا سابقاً فإن

مدققي/ات المعلومات بشر! وفي النهاية يحتفظ الجميع ببعض الآراء الشخصية في بعض المواضيع.

كخطوة أولى للوصول الى الحقيقة الموضوعية، يجب على مدققي/ات المعلومات الاعتراف بالميول الاجتماعية والسياسية عوضاً عن نكران وجودها تماماً، مع الوعي والالتزام الدائم بضرورة عدم تدخلها في عملية تدقيق المعلومات، وذلك يتحقق بإدراك المدققين/ات أو الصحفيين/ات أنّ عملية تدقيق المعلومات تتبع آلية رصينة تتمحور حول وجود دليل قوي لتأكيد أو نفي أي ادعاء، ومن هذا المنطلق يُمنع منعاً باتاً إطلاق أحكام مبنية على الآراء الشخصية أو ابتداء البحث بالقفز إلى استنتاج مبني على تحيزات أو اعتقادات معينة، عوضاً عن ابتدائه من البحث عن دليل للوصول إلى الحقيقة.

4.2. العمل تحت مبادئ موحدة:

لضمان الوصول إلى الحقيقة بكفاءة، من الضروري على مدققي/ات المعلومات اتباع مبادئ ثابتة تحول بينهم وبين أي تحيزات شخصية مثل: سياسات الشفافية وعدم التحزب، وآليات عمل محدّدة ودقيقة في التّحقق من الأخبار والمعلومات. ويجب على هذه الآليات أن تتمحور حول مبدأ وجوب إرفاق دليل بأي معلومة يتم ذكرها، والعودة إلى أصل الخبر والمصدر الأول لأي معلومة يتم التحقق من صحتها، إضافة إلى استخدام العديد من الأدوات المتاحة للتحقق من مختلف أنواع المحتوى سواء كان مقروءًا أو مرئيًا أو مسموعًا. ويجب أن يتم مراجعة هذه المبادئ والآليات بشكل دوري ومشاركتها مع الفريق للتأكيد على التزامهم بتطبيقها واتباعها.

كذلك عندما تجتمع مبادرات تدقيق المعلومات في شكل مجتمعات محلية، أو إقليمية، أو عالمية تتفق على مبادئ موحدة وتوقع عليها، فان ذلك يضمن الرقابة الذاتية والمسؤولية بين هذه المبادرات ويعزز المصداقية والنزاهة. مثال على ذلك هو مدونة المبادئ للشبكة العالمية لمدققي المعلومات IFCN ومدونة المبادئ للشبكة العربية لمدققي المعلومات AFCN.

4.3. العمل ضمن فريق متنوع

يُقترح أن يتم تدقيق المعلومات وبالذات في سياق الادعاءات السياسية الجدلية من قبل فرق مكونة من مُدَققين أو أكثر، يختلفون في الآراء والخلفيات الاجتماعية والسياسية، حيث يجب على مدققي/ات المعلومات باختلاف آرائهم ووجهات نظرهم العمل في فريق واحد كتجسيد للتوازن، ويمكن تطبيق هذه الطريقة عبر استخدام: (تدقيق المعلومات المزدوج - Double Fact checking) وهي طريقة لمراجعة مقال تدقيق المعلومات والتأكد من خلوه من أي أخطاء عبر مراجعته بشكل كامل، بتطبيق نفس الخطوات المتخذة من قبل مدقق آخر بعد تسليم المقال.

المفتاح للوصول لنتائج التفكير المعرفي -بالذات في السياق السياسي- هو تضمين ادعاءات ووجهات نظر كلا الجانبين في نفس الوقت وفي نفس التقرير، بهذه الطريقة يمكن تقليل الأخطاء الناتجة عن تضمين وجهة نظر جانب واحد فقط، حيث سيناقش مدققي/ات المعلومات ذوي وجهات النظر المختلفة نفس الأدلة لإنتاج

مقال متوازن غير متحيز لطرف دون الآخر، وهذا سيعطي القدرة للقراء على الحكم حسب مدى إقناع حجة كل جانب والتوصل إلى استنتاج أكثر استنارة مما لو تم تقديم دليل من جانب واحد فقط.

- ماذا بعد؟

يحمل المحور الأول -السابق- من دليل أنير للتحقق من المحتوى الرقمي، المعلومات الأساسية التي يجب أخذها بعين الاعتبار في تدقيق المعلومات سعيًا للوصول إلى الحقيقة.

فبعد تعرفنا على اضطراب المعلومات وتأثيراته المختلفة، وأهمية مكافحته عبر تدقيق المعلومات، وعن أنواع المحتوى المنتشر على الإنترنت ووسائل التواصل الاجتماعي. تتمحور الخطوة الثانية حول التعرف والاستعانة بالأدوات التقنية المناسبة للوصول إلى الحقيقة.

II)): المحور الثاني: الأدوات التقنية

- **من الشك إلى اليقين:**

في سيناريو معين، يبتدأ بخبر منتشر على احدى مواقع التواصل الاجتماعي. يتوقف عنده المستخدمون/ات مشككين/ات به للتحري منه، يرتابهم/ن الشك متسائلين/ات عن الطريقة المناسبة للوصول إلى اليقين.

في الحقيقة هنالك العديد من الأدوات المتاحة على الإنترنت التي يمكن أن تساعد في عملية التحقق أو التحري للوصول إلى الحقيقة، ولكن تبقى الخطوة الأولى دائماً هي الشك وعدم التصديق، يتبعها التحري والتحقق.

- أريد التحقق من مصدر صورة متداولة على وسائل التواصل الاجتماعي؟
- أريد معرفة صحة حقيقة مقطع فيديو متداول؟

للإجابة على هذه الأسئلة -وغيرها الكثير- سنقدم لكم/ن في هذه الجزئية شرحاً لأهم الأدوات والمحركات الرقمية الحديثة التي تُستخدم في التحقق والتي تساعد في الوصول إلى الحقيقة.

1. **الأدوات المفتوحة المصدر "OSINT":**

في عصر الإنترنت والثورة الرقمية، أصبح انتاج واستهلاك المعلومات أمراً لا يستغرق سوى بضع نقرات، ومع انبثاق فكرة المصدر المفتوح "Open Source" أصبح بإمكان أي شخص الوصول إلى هذه المعلومات وفحصها والتحقق منها.

الأدوات مفتوحة المصدر "OSINT" وهي اختصار لـ "Open Source Intelligence" تصنف من أهم الأدوات التقنية التي أتاحتها التكنولوجيا في إطار العمل الصحفي والاستقصائي، وهي تشير إلى جمع المعلومات والبيانات من مصادر مفتوحة وعامة مثل الإنترنت ووسائل الإعلام الاجتماعية والمنتديات، والمدونات، والمواقع الحكومية، والعامة. تعتبر الأدوات المفتوحة المصدر أدوات قوية للتحقق من المحتوى وتتيح الوصول للعديد من المعلومات التي يمكن استخدامها لفهم السياق المحتمل لحالات التحقيق.

أهمية الأدوات المفتوحة المصدر

تلعب الأدوات المفتوحة المصدر دورًا مهماً في عملية جمع وتحليل المعلومات والتحقق من المحتوى، وتوفر مجموعة واسعة من الطرق والتقنيات لتحقيق ذلك. ففي بعض الأحيان وعند انتشار خبر متداول بشكل واسع وسريع، يمكن ألا يكون البحث الاعتيادي كافياً للعثور على مصدر الخبر وحقيقته، لذا أصبح استعمال هذه الأدوات وفهم كيفية عملها وآلية استخدامها أمرًا ضروريًا لمدققي/ات المعلومات وللسعاة نحو الحقيقة.

- ومن أمثلة هذه الأدوات:
- محركات البحث بأنواعها.
- وسائل التواصل الاجتماعية.
- خدمات التحقق من المواقع الجغرافية.
- منتديات ومجتمعات الإنترنت.
- **ملاحظة:**

للاطلاع على المزيد حول الأدوات المفتوحة المصدر يمكن زيارة موقع "OSINT Framework" الذي يهتم بجمع الأدوات والمواقع المجانية وتصنيفها حسب الاستخدام.

محركات البحث

محركات البحث هي أدوات على الإنترنت تسمح للمستخدمين/ات بالبحث عن المحتوى والمعلومات عبر الويب. تقوم هذه المحركات بفهرسة الصفحات والمواقع على الإنترنت وتقديم النتائج المناسبة لاستفسارات البحث التي يدخلها المستخدمون/ات.

- تعمل محركات البحث عادة من خلال عمليتين رئيسيتين:

- **عملية الفهرسة:**

أثناء هذه العملية، تقوم محركات البحث بزيارة صفحات الويب -التي يُسمح لها بدخولها- وجمع المعلومات عنها عبر عناكب البحث "Web crawlers"، ثم تخزن هذه المعلومات في قواعد بيانات تعرف بالفهرس.

- **عملية البحث ذاتها:**

خلال عملية البحث، يتم تحليل الاستفسارات أو الكلمات المفتاحية التي يبحث عنها المستخدمون/ات ومقارنتها بالمعلومات التي سبق وتم تخزينها في الفهرس الخاص بمتصفح البحث، ومن ثم يتم تقديم قائمة من الروابط والصفحات التي تتوافق مع متطلبات المستخدم.

- **محركات البحث لا تقوم بأرشفة كل المواقع**

لا تؤرشف محركات البحث كل مواقع الإنترنت، هذا الأمر يعتمد على إعدادات الموقع في حد ذاتها وهل تم السماح من قبل الموقع بأرشفته وظهوره في نتائج المتصفحات أم لا.

- **الإنترنت السطحي فقط**

بشكل عام، تعمل محركات البحث الاعتيادية بالبحث على صفحات الإنترنت السطحي "Surface Web" وهي الصفحات المتاحة للعامة والتي لا تتطلب كلمات مرور أو طرق حماية للوصول إليها، على عكس البريد الالكتروني -على سبيل المثال- الذي يتطلب كلمة سر للوصول إليه، فمثل هذه البيانات تعتبر جزء من الإنترنت العميق "Deep Web". أيضاً، لا يمكن لهذه المتصفحات الاعتيادية الوصول أو البحث عن المحتوى الموجود على مواقع الإنترنت المظلم "Dark Web" باعتباره جزء من الإنترنت العميق.

- **نتائج البحث والموثوقية**

يجب الأخذ في الحسبان بأن المحتوى المتواجد على شبكة الإنترنت هو أيضاً مصنوع من قبل بشر، حيث يحتمل أن يكون صحيحًا أو زائفًا، ولهذا ليست كل نتائج متصفحات البحث صحيحة، بل يجب الاعتماد على أخذ المعلومات من مواقع موثوقة وأصيلة.

- **نتائج البحث والاستهداف الصحيح**

تعتمد احتمالية وصولنا للنتيجة المطلوبة خلال البحث عبر محركات البحث على العديد من العوامل. من أهمها "الاستهداف الصحيح" أو "استعمال الكلمات المفتاحية الصحيحة"، إذ يجب على المستخدم التفكير في الكلمات المفتاحية المناسبة، والتي تتمحور حول الموضوع المراد البحث عنه، واستخدام الأدوات المتاحة للفلترة للحصول على نتائج بحث أكثر دقة.

- **محركات البحث: متشابهة، ولكنها مختلفة**

تؤدي أغلب محركات البحث نفس الوظيفة أو الغرض، ولكن تختلف في العديد من الميزات، لعل أبرزها الخصائص التي تقدمها لفلترة المحتوى وللبحث الفعال. ولكن الخطوة الأولى في البحث على مختلف محركات البحث هي الاستهداف الصحيح للكلمات المفتاحية وقدرة التفكير والتعبير الصحيحة عن المعلومات المراد البحث عنها.

تستخدم محركات البحث خوارزميات خاصة لفهرسة البيانات وربطها، لذلك يكون لكل محرك طريقة بحث خاصة به للعثور على ما يحاول المستخدمون/ات البحث عنه، ولأن كل محرك بحث يستخدم خوارزميات مختلفة عن المحركات الأخرى؛ ينتج عن كل محرك نتائج بحث تختلف قليلاً عن محركات البحث الأخرى.

1.1. البحث المتقدم على محرك البحث جوجل "Google"

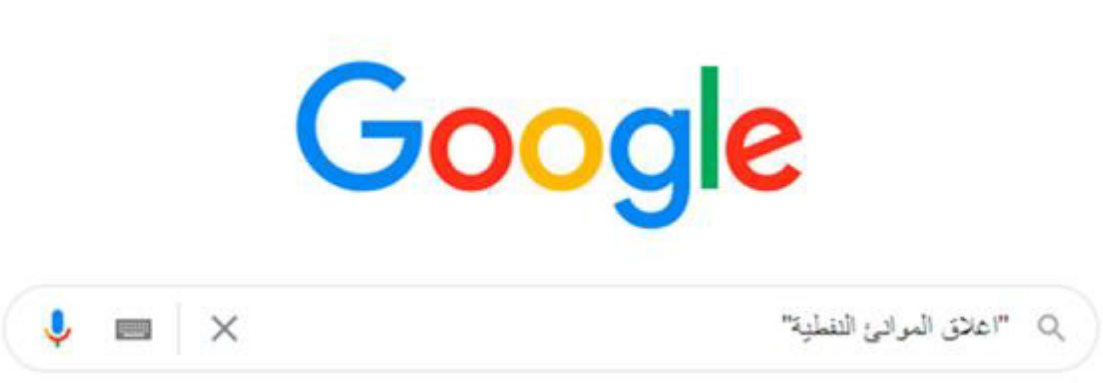
خلال عملية البحث باستخدام محرك البحث جوجل، هناك مجموعة من الآليات والأدوات التي من شأنها مساعدتنا في إظهار نتائج دقيقة والتي يمكن تخصيصها والتحكم فيها لتسريع الوصول للمحتوى أو الخبر المراد البحث عنه.

1.1.1. تخصيص فترة زمنية محددة:

يتيح هذا الخيار إظهار نتائج البحث ضمن فترة زمنية محددة، حيث يمكن البحث باستخدام فترة زمنية محددة عبر الضغط على خيار "الأدوات"، ثم من قائمة "أي وقت" يمكن تحديد الفترة الزمنية التي نريدها. وللحصول على المزيد من الخيارات يمكن استعمال الخيار "نطاق مخصص" والذي يمكن المستخدم من تحديد فترة زمنية مخصصة من القائمة المنسدلة: يوم، أو شهر، أو سنة، أو فترة محددة (من – إلى).

1.1.2. "البحث الحرفي" عن كلمة أو جملة محددة: [13] [14]

يتيح هذا الخيار إظهار نتائج البحث التي تحتوي الكلمات أو الجمل المحددة التي نريدها فقط، عبر وضع الكلمة أو الجملة المراد البحث عنها داخل علامتي تنصيص " ". لن يظهر محرك البحث أي نتيجة ما لم تحتو على الكلمات التي تم وضعها بين علامتي التنصيص.

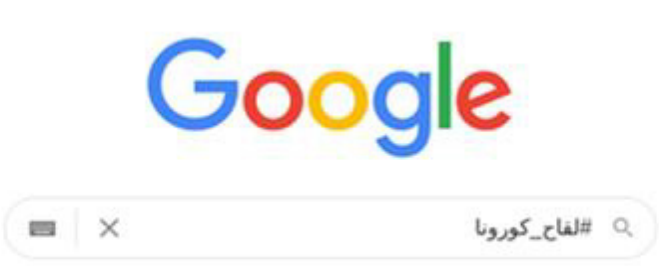


1.1.3. تخصيص البحث ضمن موقع إلكتروني محدد:

يتيح هذا الخيار البحث بشرط أن تكون نتائج البحث مقتصرة على موقع محدد. على سبيل المثال: للبحث عن المواضيع أو المواد التي تتحدث عن "بلدية زليتن" في موقع "اللجنة المركزية لانتخابات المجالس البلدية "، نكتب عبارة "بلدية زليتن" ثم نُرفقها بكلمة :site ثم نضع عنوان موقع "اللجنة المركزية لانتخابات المجالس البلدية" "Ccmce.ly".

1.1.4. تخصيص البحث عن وسم "**Hashtag**" محدد:

يتيح هذا الخيار البحث عن "وسم" معين يُستخدم على وسائل التواصل الاجتماعي أو في مواقع إلكترونية. على سبيل المثال: للبحث عن المواقع والمنشورات التي تناولت وسم "لقاح كورونا"، نكتب في حقل البحث #لقاح_كورونا.



1.1.5. طرق أخرى:

1.1.5.1. استثناء الكلمات: يمكن استخدام إشارة الطرح (-) لاستثناء كلمة أو جملة من نتائج البحث. على سبيل المثال: لاستثناء سيارات فورد "Ford" وإظهار النتائج المتعلقة بالعلامة التجارية "Tom Ford" فقط، نكتب (Tom Ford -Motors).

1.1.5.2. البحث عن شخص/شركة معينة: يمكن استخدام إشارة (@) للبحث عن شخص معين أو شركة معينة على وسائل التواصل الاجتماعي، وذلك بكتابة معرفه الرقمي بعد إشارة @ في محرك البحث.

1.1.5.3. ملء الفراغات: يمكن استخدام إشارة النجمة (*) للبحث عن العبارات أو الكلمات التي قد يكون المستخدمون/ات قد نسوها في جملة معينة. على سبيل المثال: في حالة نسيان كلمة "المحتوى" أو "المعلومات" في سياق جملة (تدقيق المعلومات أنير)، نضع نجمة مكان الكلمة المنسية (تدقيق * أنير).

1.1.5.4. نوع الملف: يمكن استخدام معامل نوع الملف (filetype:) للبحث عن ملفات محددة من نوع معين. على سبيل المثال: للبحث عن دليل أنير للسلامة الرقمية بصيغة "PDF" نكتب (filetype:pdf دليل أنير للسلامة الرقمية).

1.1.5.5. تعريف الكلمة: يمكن استخدام معامل القاموس (define:) للبحث عن تعريف أو معنى كلمة محددة. على سبيل المثال: للبحث عن تعريف كلمة "Fact-Checking" نكتب (define:Fact-Checking).

- **ملاحظة:**

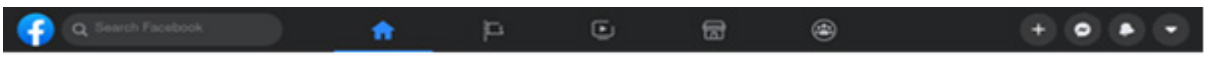
للتعرف على بقية طرق البحث المتقدم على محرك بحث جوجل يمكن زيارة الصفحة المخصصة لذلك على الموقع الخاص بمحرك البحث.

1.2. البحث المتقدم على فيسبوك "Facebook"

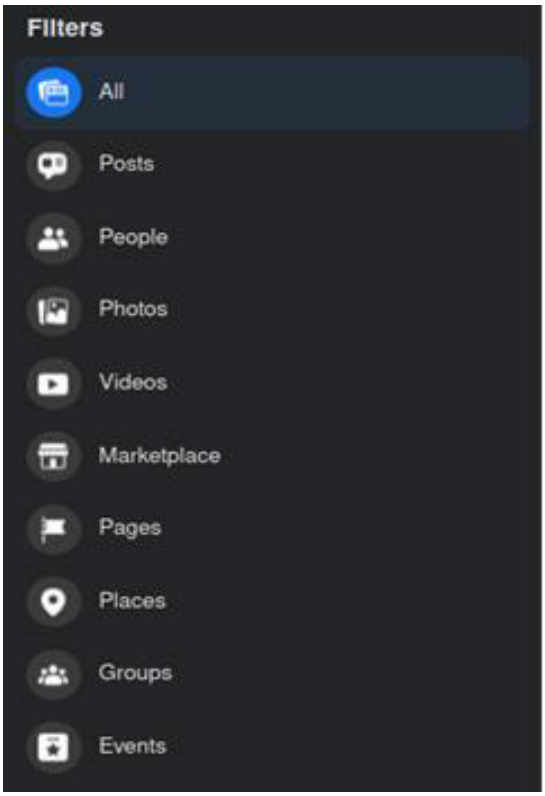
كما هو الحال على محرك بحث جوجل، تتيح منصات التواصل الاجتماعي ومنها فيسبوك إمكانية البحث داخل المنصة.

1.2.1. البحث ضمن كامل موقع فيسبوك:

وذلك من خلال خيار البحث أعلى الصفحة في حقل البحث، عبر إدخال الكلمة أو الجملة المفتاحية المراد البحث عنها ضمن حقل البحث.



كما يمكن تخصيص البحث ضمن الخيارات الظاهرة في الصورة التالية:

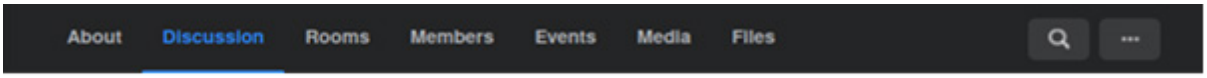


1.2.2. البحث داخل صفحة "Page":

يمكّن هذا الخيار من البحث ضمن محتوى صفحة محددة على فيسبوك. عبر خيار البحث (أيقونة المكبر) أعلى الصفحة.

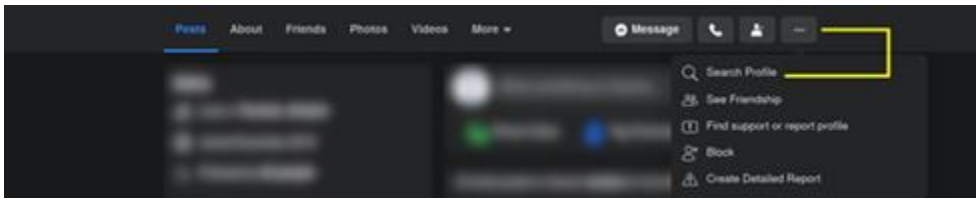
1.2.3. البحث داخل مجموعة "Group":

يمكّن هذا الخيار من البحث ضمن محتوى مجموعة محددة. عبر خيار البحث (أيقونة المكبر) أعلى المجموعة.



1.2.4. البحث داخل حساب شخصي:

يمكّن هذا الخيار من البحث ضمن حساب شخصي، وذلك بالنقر على علامة النقاط في الملف الشخصي (...) ومن ثم اختيار علامة البحث (أيقونة المكبر) ضمن القائمة المنسدلة.



2. التحقق من المحتوى المرئي

2.1. التحقق من الصور

عند تصفح الإنترنت أو في حال قيام صديق لك بإرسال صورة معينة أو مصادفتك إياها في مواقع التواصل الاجتماعي في سياق معين، قد ينتابك الشك من حقيقة ارتباط هذه الصورة بالسياق المذكور في الادعاء، باستخدام هذه الأدوات الموثوقة يمكنك التحقق من حقيقة الصور، وفي بعض الأحيان قد تصل إلى مصدرها الأصلي، وبذلك ستمتلك القدرة على معرفة مصدرها الحقيقي أينما كُنت.

2.1.1. البحث العكسي عن الصور

البحث العكسي "Reverse Image Search" هو عملية بحث تبدأ بالصور عوضاً عن الكلمات المفتاحية، يتم فيها البحث عن نفس الصورة أو الصور المشابهة لها، وذلك بغرض الوصول للمزيد من المعلومات عنها، مثل: الناشر الأصلي وتاريخ انتشارها والسياق الجغرافي المرتبط بها والمصدر الحقيقي لها. قد تختلف نتائج البحث العكسي من محرك بحث إلى آخر بناء على جودة الصور المستخدمة خلال عملية البحث، وآلية عمل الأداة، واحتمالية تواجدها في قواعد بيانات كل أداة.

- **متى نستخدم البحث العكسي؟**

- **التحقق من صحة الصور:**

يمكننا استخدام البحث العكسي للتحقق من صحة الصور المتداولة على الإنترنت، والتأكد مما إذا تم التلاعب بها.

- **اكتشاف مصادر الصور:**

يمكننا استخدام البحث العكسي للعثور على مصادر الصور المطلوبة والمعلومات المتعلقة بها.

- **العثور على صور ذات صلة:**

يمكننا استخدام البحث العكسي للعثور على صور مشابهة تتعلق بحدث معين وتساعد في إيضاح المحتوى المطلوب.

- **الحصول على معلومات إضافية:**

يمكننا استخدام البحث العكسي في العثور على معلومات إضافية حول الصور وتوفير نتائج مرتبطة بشكل أساسي للصور.

- فائدة البحث العكسي للصور

باستخدام المعلومات المتحصل عليها عن طريق البحث العكسي، يمكن للمستخدم معرفة حقيقة صورة معينة وبالتالي الحصول على دليل لإثبات أو نفي الأخبار المتعلقة بها. مثلاً: في حالة تداول صورة في سياق معين وبعد البحث عنها نجد أنها صورة متواجدة على الإنترنت بتاريخ قديم وفي سياقات أخرى، يمكننا نفي الادعاء وإثبات بطلان الأخبار المتداولة عنها في الوقت الحالي.

2.1.1.1. محرك بحث جوجل "[15] Google Image Search"

تتم عملية البحث العكسي باستخدام الصورة المراد التحقق منها نفسها، حيث يقوم المستخدم بفتح موقع المحرك الخاص بالصور وتحميل الصورة أو إدخال عنوان (URL) الخاص بها والبحث عنها. قد تُظهر النتائج الصورة نفسها أو صور مماثلة لها، بالإضافة إلى مواقع أو صفحات قد استخدمت نفس الصورة من قبل.

- البحث العكسي عن الصور باستخدام رابط الصورة المراد البحث عنها:

- الدخول على الموقع الخاص بالبحث العكسي لجوجل.
- ثم الضغط على أيقونة الكاميرا:

- بعد ذلك، لصق رابط الصورة (URL) في الحقل المخصص:

- البحث العكسي عن الصور باستخدام صورة متوفرة لدينا:

- الدخول على الموقع الخاص بالبحث العكسي لجوجل.
- ثم الضغط على أيقونة الكاميرا:

- بعد ذلك، الضغط على خيار "تحميل ملف":

- اختيار الصورة المراد البحث عنها.

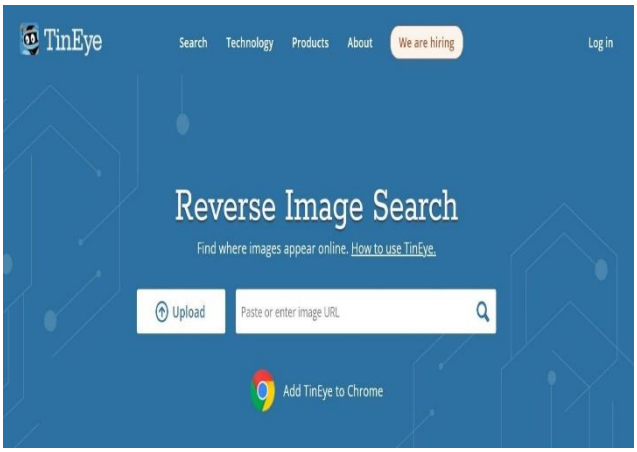
2.1.1.2. أداة "Tineye" [16] [17]

أداة "Tineye" هي إحدى الأدوات الفعالة للبحث العكسي للصور، تتميز هذه الأداة بدقتها وفعاليتها وحيازتها على قاعدة بيانات كبيرة تحتوي على ملايين الصور مما يسهل عملية البحث العكسي.

تستخدم أداة "Tineye" قاعدة بيانات خاصة بها، يتم تجميع بياناتها عن طريق استعراض محتويات شبكة الإنترنت من الصور ووضع توقيع فريد لكل صورة. عند البحث عن صورة معينة باستخدام هذه الأداة يتم إنشاء توقيع رقمي فريد لها باستخدام تقنيات التعرف على الصور، ويتم مقارنة هذا التوقيع مع كل التوقيعات الأخرى المتواجدة في قاعدة بيانات الأداة للعثور على توقيع مطابق.

على خلاف البحث العكسي باستخدام جوجل، في العادة لا تستعرض أداة "Tineye" الصور المشابهة، وإنما يتم العثور على تطابقات الصور بما في ذلك الصور التي تم تقليصها أو تحريرها أو تغيير حجمها.

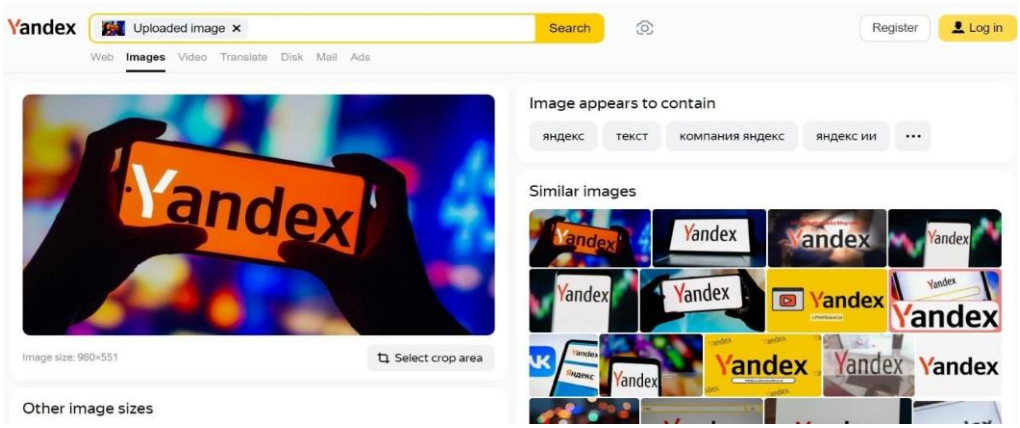
- البحث العكسي عن الصور باستخدام "**Tineye":**



- الدخول على الموقع الخاص بالأداة.
- رفع الصورة المراد البحث عنها.

2.1.1.3. محرك بحث " Yandex Images" [17] [18]

يعتبر محرك بحث ياندكس الروسي أحد أهم محركات البحث العكسي الخاص بالصور، حيث يمتاز بنتائج دقيقة في العديد من الأحيان.



- البحث العكسي عن الصور باستخدام "**Yandex Images":**

- الدخول على الموقع الخاص بالأداة.
- رفع الصورة المراد البحث عنها أو إرفاق رابط الـURL الخاص بها.

2.1.1.4. محرك بحث "Bing" [19]

يعد محرك بحث "Bing" أحد أشهر محركات البحث والذي يتبع شركة مايكروسوفت. ويوفر خدمات البحث العكسي عن الصور.

- البحث العكسي عن الصور باستخدام "**Bing":**

- اختيار أيقونة الكاميرا.
- رفع الصورة المراد البحث عنها أو إرفاق رابط الـURL الخاص بها.

2.1.2. التحقق من التلاعب في الصور

في بعض الأحيان، قد لا تفيد طرق البحث العكسي عن الصور؛ وذلك بسبب كون الصورة في حد ذاتها مفبركة أو قد تم التعديل عليها باستخدام أحد برامج تعديل الصور مثل برنامج "Photoshop" الشهير. ولهذا السبب يمكننا استخدام أدوات تحليل الصور للكشف عن التلاعب والتعديلات.

2.1.2.1. أداة "Forensically": [18] [20]

أداة "Forensically" هي أداة متقدمة تستخدم لتحليل الصور الرقمية بهدف اكتشاف التلاعب والتعديل عليها. يمكن استخدام هذه الأداة للمساعدة في التحقق من صحة الصور والكشف عن أي تغييرات أو تلاعب أجري عليها، وتستند على مجموعة من المعادلات الرياضية والإحصائية وعلم الكمبيوتر لتحليل الصور بطرق معقدة.

تحتوي الأداة على العديد من البرامج التعليمية لمساعدة المستخدمين/ات في الحصول على المزيد من المعلومات حول كيفية تحليل ما يتم مشاهدته، بالإضافة إلى ذلك، فهو فعالٌ لأنه يوفر بيانات دقيقة بخصوص الصور المحررة والمعدلة بالفوتوشوب وذلك باستخدام خوارزمية معينة لمعرفة ما إذا كانت الصورة قد تم تعديلها باستخدام برنامج فوتوشوب أم لا. في حال تم تعديل الصورة بالفوتوشوب أو تحريرها، فيمكن ملاحظة اللون في تحليل الصورة.

- توفر أداة "**Forensically**" مجموعة متنوعة من الأدوات التي يمكن استخدامها لكشف التلاعب في الصور. من بينها:

- **Error Level Analysis" (ELA)":**

تستخدم ELA لتحليل الفروق في مستويات الخطأ بين مناطق مختلفة في الصورة. إذا تم تعديل جزء معين من الصورة، ستظهر فروق في مستوى الخطأ بالمقارنة مع الأجزاء الأصلية.

- **"Noise Analysis":**

تحليل مستوى الضوضاء في الصورة يمكن أن يكشف عن أي تلاعب بها. التلاعبات غالبًا ما تؤدي إلى إضافة نمط معين من الضوضاء أو تغييرات في مستوى الضوضاء.

- **"Clone Detection":**

تساعد في اكتشاف مناطق متشابهة أو مكررة في الصورة، مما قد يشير إلى عمليات نسخ ولصق للعناصر أو التلاعب بها.

- **"Metadata Analysis":**

تحليل البيانات الوصفية المدرجة في الصورة (مثل التوقيت والكاميرا المستخدمة) يمكن أن يكشف عن أي تلاعب تم في تواريخ التصوير أو الكاميرا المستخدمة.

- **"Pixel Analysis":**

يقوم بتحليل البكسلات في الصورة للكشف عن أي تغييرات غير مألوفة أو غير طبيعية.

- استخدام أداة "**Forensically":**

- الدخول على الموقع الخاص بالأداة.
- رفع الصورة المراد تحليلها.
- اختيار الأداة المراد استخدامها.

- أدوات أخرى للتحقق من التلاعب في الصور:
  - أداة "FotoForensics"."
  - أداة Ghiro.

2.2. التحقق من مقاطع الفيديو

تعد عملية التحقق من مقاطع الفيديو أكثر تعقيداً من عملية التحقق من المحتوى النصي أو الصور. إذ يصعب في بعض الأحيان تعقب المصدر الأصلي للعديد من الأسباب مثل التلاعب بأجزاء من الفيديو ووضعها في سياق آخر تماماً.

- يهدف التحقق من الفيديو إلى عدة أمور، منها:
  - معرفة تاريخ نشره لأول مرة.
  - معرفة سياقه.
  - معرفة ما إذا كان قد تم اجتزاءه.
  - معرفة معلومات عن محتواه وعناصره.

- قبل البدء في التحقق من الفيديو يجب الأخذ بعين الاعتبار:
  - هل تم نشره من قبل وسائل إعلامية موثوقة؟
  - هل يحمل شعاراً معيناً؟
  - ما هي اللهجة واللكنة المتداولة فيه؟
  - هل هناك لافتة أو أسماء تجارية تظهر فيه؟
  - هل هناك مبنى أو مقر شهير يظهر فيه يمكن من خلاله التحقق من الموقع بواسطة صور الأقمار الصناعية؟
  - ما هي تضاريس الطقس وهل تتوافق مع المنطقة التي يُنسب لها المقطع؟
  - هل ما جاء في المقطع منطقي بحسب السياق المنسوب له؟

2.2.1. البحث عن مقاطع الفيديو باستخدام الكلمات المفتاحية [21]

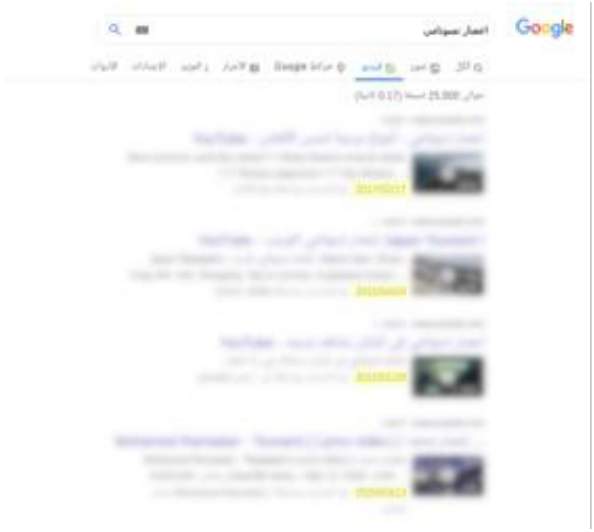
يتم استخدام محركات البحث التي تستعرض نتائج مقاطع الفيديو فقط في هذه الطريقة، وذلك عبر تحليل محتوى الفيديو بدقة والانتباه لكل التفاصيل التي يجب أن تؤخذ بعين الاعتبار. بعد ذلك، يتم وضع قائمة من الكلمات المفتاحية المتعلقة بمحتوى الفيديو والمبنية على أحداثه ليتم استخدامها في محركات البحث بهدف الوصول إلى معلومات أكثر عنه أو عن مصدره الأصلي.

- البحث عن مقطع فيديو باستخدام الكلمات المفتاحية:

- الدخول على الموقع الخاص بالبحث عن الفيديو هات لجوجل.

- إدخال الكلمات المفتاحية أو الكلمات الدالة على الفيديو.

سيقوم المحرك بعرض تاريخ نشر الفيديو حسب نتائج البحث الظاهرة، كما يتيح المحرك خاصية البحث ضمن فترات زمنية محددة أيضاً. يجب التنويه إلى أن نتائج البحث السابقة لا تعني بالضرورة أن الفيديو تم نشره لأول مرة في ذلك الزمان.



2.2.2. البحث عن الفيديو باستخدام موقع يوتيوب "Youtube"

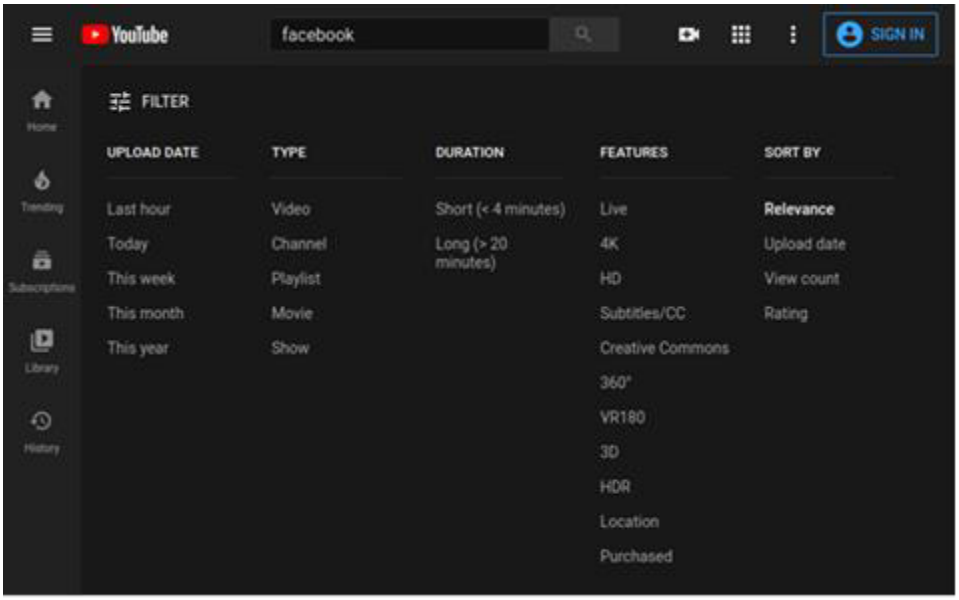
يعتبر موقع يوتيوب أكبر موقع خاص بالفيديوهات في العالم. يمكن استغلال هذه المعلومة في البحث عن الفيديو المطلوب عن طريق هذا الموقع عبر استخدام الحقل الخاص بالبحث داخل الموقع.

- البحث عن مقطع فيديو باستخدام "Youtube":

- الدخول على موقع "Youtube".

- إدخال الكلمات المفتاحية أو الكلمات الدالة على الفيديو في حقل البحث.

- بعد البحث، يمكن تخصيص البحث عبر مجموعة من خيارات التصفية أسفل حقل البحث.



- **الخيارات المتاحة:**

- **تاريخ التحميل "Upload date":**

يمكن من خلاله تحديد الفيديوهات التي رُفعت في فترة زمنية معينة.

- **النوع "Type":**

يمكّن من خلاله تحديد هل الكلمة أو الكلمات التي تم إدخالها في حقل البحث تتبع: فيديو، أو قناة، أو قائمة تشغيل، أو فيلم.

- **المدة "Duration":**

يمكن من خلاله تحديد ما إذا كانت الفيديوهات المراد إظهارها في نتائج البحث مدتها أقل من 4 دقائق أو أكثر من 20 دقيقة.

- **المزايا "Features":**

تحتوي مجموعة من المزايا مثل: الفيديوهات ذات البث المباشر، الفيديوهات التي تحتوي على ترجمة، وغيرها من الخيارات الموضحة في الصورة السابقة.

- **الفرز "Sort":**

يمكن من خلاله ترتيب نتائج البحث بناءً على: تاريخ التحميل، أو عدد المشاهدات، أو التقييم.

- أداة **"Youtube DataViewer":**

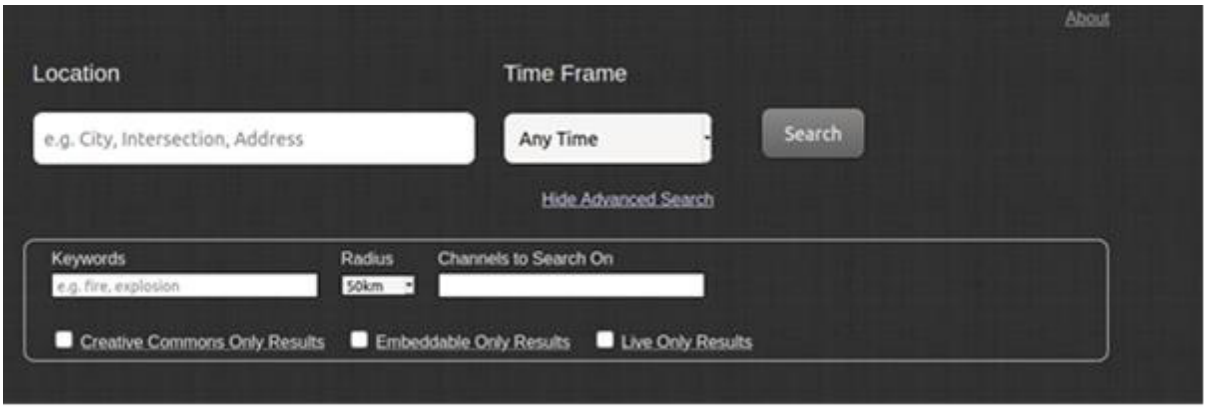
"Youtube DataViewer" هي أداة من تصميم منظمة العفو الدولية، يمكن استعمالها لكشف البيانات الوصفية للمقاطع التي يتم رفعها على يوتيوب. في هذا السياق، يمكن استعمالها بعد الوصول للفيديو المطلوب في حالة تواجده على يوتيوب، للحصول على المزيد من البيانات حوله.

- أداة **"Geo-Search-Tool":**

"Geo-Search-Tool" هي أداة تتيح إمكانية البحث واستعراض الفيديوهات التي رُفِعت على منصة يوتيوب من منطقة أو دولة معينة خلال فترة زمنية محددة.

على سبيل المثال: باستخدام هذه الأداة، يمكننا البحث عن الفيديوهات التي تم رفعها فقط من ليبيا خلال فترة زمنية معينة وباستخدام كلمات مفتاحية محددة. وهكذا نتائج البحث ستتمحور فقط حول: (الموقع الجغرافي الذي تم رفع الفيديو منه - الفترة الزمنية المحددة - الكلمات المفتاحية).

- استخدام أداة "**Geo-Search-Tool**" للبحث عن الفيديوهات التي رُفعت من منطقة أو دولة



محددة:

- الدخول على الموقع الخاص بالأداة.
- ملء الحقل الخاص بالموقع الجغرافي "Location".
- تحديد الفترات الزمنية المطلوبة عبر "Time Frame".
- ملء الحقل الخاص بالكلمات المفتاحية "Keywords".
- الضغط على زر البحث.

2.2.3. البحث باستخدام صورة من فيديو [22]

يعتمد استخدام هذه الطريقة على تجزئة أو تقطيع الفيديو إلى عدة لقطات للحصول على صورة ثابتة، فعندما لا يتوفر اسم الفيديو أو يفشل البحث باستخدام الكلمات المفتاحية على محركات البحث المختلفة أو على موقع يوتيوب، يمكننا اللجوء إلى استخدام أحد برامج تحرير الفيديو لاقتطاع لقطة معينة "Frame"، ومن ثم وضع هذه اللقطة في محركات البحث العكسي للصور.

- **كيفية استخدام البحث بصورة من فيديو:**

- اقتطاع لقطة واضحة من الفيديو باستخدام برامج تحرير الفيديوهات أو عن طريق أخذ لقطة شاشة واضحة.
- وضع اللقطة التي تم التقاطها في محركات البحث العكسي الخاصة بالصور.

اثنان في واحد: أداة "**InVid**" للتحقق

- طرق أسهل للتحقق من المحتوى المرئي

قمنا بالإشارة سابقاً إلى مجموعة من الأساليب التي يمكن استخدامها للتحقق من المحتوى المرئي، سواء كان صورًا أو فيديوهات. ولكن في بعض الأحيان، قد تتعقد عمليات البحث والتحقق وتستغرق وقتًا طويلًا، خاصةً إذا كنا نحاول استخدام أكثر من أداة في آن واحد. فما هي أفضل خياراتنا في هذه الحالة؟

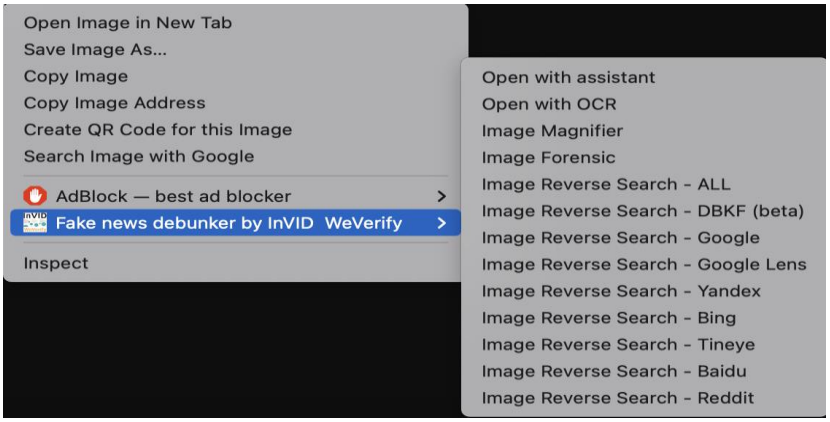
2.3 أداة "InVid" [23]

"InVid"" هي أداة مساعدة في عمليات التحقق من الصور والفيديوهات، توفر العديد من المزايا والخاصيات التي تسهل عملية التحقق وتختصر الوقت، سواء في عمليات البحث العكسي أو في التحقق من مقاطع الفيديو وتجزئتها وغيرها.

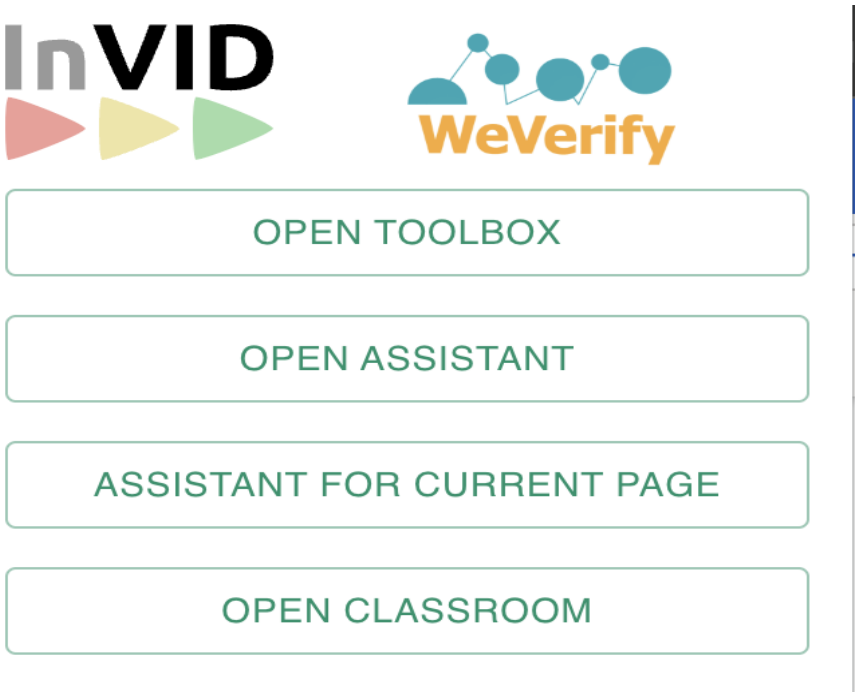
- **اختصار للوقت والجهد:**
- تتيح أداة "InVid" إمكانية البحث العكسي للصور على أكثر من 7 محركات بحث عكسي في نفس الوقت عن طريق نقرتين فقط.
- تتيح أداة "InVid" خصائص تحليل التلاعب في الصور وتكبير التفاصيل فيها وإمكانية التعرف واستخراج الكلام من الصور "OCR" عن طريق نقرتين فقط.

- ويمكن أيضاً عن طريقها إجراء العديد من العمليات مثل:
- تحليل الفيديوهات "Video Analysis"
- تقسيم مقاطع الفيديو إلى لقطات "Frames"
- تحليل البيانات الوصفية لمقاطع الفيديو وبيانات حقوق الملكية.
- إمكانية البحث المتقدم على منصة تويتر.
- إتاحة محرك بحث خاص بتقارير تدقيق المعلومات.
- إمكانية إجراء تحليل شبكات "Social network anaylsis".

- استخدام أداة "**InVid**":
- تحميل الأداة كإضافة على المتصفح من الموقع الرسمي وتثبيتها.
- بعد تثبيتها:
  - ستظهر قائمة البحث السريع في القائمة المنسدلة عند الضغط على زر الفأرة الأيمن.



- ستظهر أيقونة الأداة والتي يمكن الضغط عليها للوصول لباقي الأدوات واستعمالها.



3. بيانات الموقع الجغرافي

بيانات المواقع الجغرافية لها أهمية كبيرة جداً في عمليات تدقيق المعلومات، ففي بعض الأحيان تفشل وسائل التحقق من المحتوى المرئي في الوصول إلى المصدر الأصلي. في مثل هذه الحالات، يمكننا الاستعانة بتطبيقات وخدمات المواقع الجغرافية، وبالتركيز على التفاصيل الدقيقة الموجودة في الصورة أو الفيديو، يمكن استخراج بعض العلامات الدالة والوصول إلى أدلة قاطعة تنفي أو تؤكد حقيقة ادعاء معين.

- **نقاط مهمة عند استخدام أدوات التحقق من الموقع الجغرافي:**

- الانتباه لأدق التفاصيل في الصور أو الفيديوهات:
  - أسماء اللافتات أو المحلات أو الشوارع واللغة المستخدمة.
  - التحقق من وجود أعلام دولة معينة.
  - الانتباه لطبيعة ملابس الناس (صيفي أم شتوي).
  - الانتباه لحالة الطقس والجو العام.
  - الانتباه للعبارات واللغة المتحدث بها في الخلفية.

- التضاريس كالجبال والوديان والتلال.
- طراز المباني والنوافذ والشرفات.
- الأحداث المتزامنة وقت حدوث الادعاء.

- **مقارنة مكان الحدث المذكور في الادعاء مع صوره المرفقة في أدوات الموقع الجغرافي.**

مع مراعاة جميع هذه النقاط، تتاح لنا مجموعة واسعة من الأساليب للتحقق من صحة ادعاء معين باستخدام البيانات الجغرافية التي قمنا بجمعها عبر المراقبة والتحليل. يُمكن استخدام هذه البيانات فيما بعد للبحث عن اسم محل معين أو عبارات معينة تم ملاحظتها.

3.1 "Google Maps": [22]

أداة "Google Maps" هي خدمة مقدمة من شركة جوجل، وهي مجموعة من الخرائط تتيح للمستخدمين/ات البحث عن مواقع معينة والحصول على توجيهات للوصول إليها. كما تتيح خاصية عرض الخرائط بشكل ثنائي وثلاثي الأبعاد (حسب المنطقة والتفاصيل) وتتضمن معلومات عن المحلات التجارية والمعالم وغيرها.

3.2 "Google Earth": [24]

أداة "Google Earth" هي خدمة مقدمة من شركة جوجل على شكل تطبيق يتيح للمستخدمين/ات استكشاف كوكب الأرض، باستخدام تقنية الصور الجوية والأقمار الصناعية. يمكن استخدام هذه الأداة لعرض الصور المأخوذة من الفضاء واستكشاف بيانات جغرافية متقدمة، وعرض ومقارنة صور الأقمار الصناعية عبر عدة سنوات.

3.3 "NASA Earth Observatory": [25]

أداة "Earth observatory" مرصد الأرض" المقدمة من قبل وكالة الفضاء الأمريكية (ناسا)، هي منصة لمشاركة صور الأقمار الصناعية والمعلومات المتعلقة بالطقس والبيئة. تقسم الأداة الصور الاصطناعية التي توفرها إلى عدة فئات، منها: المياه، الثلوج والجليد، الحرارة، وغيرها. كما يمكن اختيار السنة المراد البحث فيها.

3.4 "Wikimapia":

أداة "Wikimapia" هي موقع للخرائط مثل خرائط Google، ولكن يختلف عنه في كونه خريطة مفتوحة المصدر؛ أي يمكن للمستخدمين/ات إضافة أماكن وكتابة شروحات لهذه الأماكن، بمعنى أنه يعتمد على الحشود لإضافة البيانات. كما يتضمن إشارات وتوصيفات للمعالم الجغرافية.

3.5 "Google Translate": [22]

خدمة "Google Tranlslate" هي خدمة ترجمة مقدمة من قبل شركة جوجل. يمكن للمستخدم في سياق تدقيق المعلومات استعمال خدمة "Google Translate" لتسهيل وتسريع العمل، عبر ترجمة النص أو عبر خاصية ترجمة النص من الصور. يمكن استخدام هذه الخدمة في العديد من السياقات مثل: ترجمة اللافتات المكتوبة بلغات أخرى، أو الأخبار المحلية المنشورة بمختلف اللغات، أو للتأكد من صحة ترجمة معلومة ما.

4. بيانات مواقع الويب

تعتبر مواقع التواصل الاجتماعي بيئة خصبة لانتشار المعلومات الخاطئة والمضللة، ومع هذا لا يقتصر وجود مثل هذه المعلومات على مواقع التواصل الاجتماعي فقط. توجد العديد من المواقع على شبكة الإنترنت التي تساهم في اضطراب المعلومات، وقد ترتبط بعض المعلومات الخاطئة أو المضللة على مواقع التواصل بمواقع الكترونية يشار لها كمصادر رسمية.

تتجلى هنا أهمية التحقق من بيانات مواقع الويب والتأكد من موثوقية المواقع التي نستقي منها المعلومات.

فكيف يمكننا التحقق من بيانات هذه المواقع بحد ذاتها؟ وكيف نستطيع إثبات موثوقيتها؟

يمكن بكل تأكيد استخدام كل طرق البحث التي تطرقنا لها سابقاً مثل البحث العكسي عن الصور أو استخدام محركات البحث في تدقيق المعلومات الموجودة على المواقع بغرض الوصول للحقيقة. ولكن لتحديد موثوقية الموقع بحد ذاته، يمكن استخدام أدوات متخصصة في استخراج بيانات المواقع الالكترونية، ليتحقق المستخدمين/ات منها بدوره ويحدد مدى موثوقية الموقع من عدمه.

4.1 امتداد الدومين "Domain Extension": [26]

امتداد الدومين هو الجزء الأخير من عنوان موقع معين على الإنترنت والذي يظهر بعد النقطة في عنوان الـ URL. يرتبط هذا الجزء في العادة بنوع الموقع أو موقعه الجغرافي.

- لامتدادات الدومين العديد من التصنيفات، منها:

- امتدادات دومين المستوى العالي **(gTLDs) (Genereic Top-Level Domains)**: هذه هي الامتدادات التي تشمل الأشكال الشهيرة والتي يمكن استخدامها لأي موقع حول العالم.

- **org**: ترتبط بالمؤسسات غير الربحية والمنظمات. مثل: Wikipedia.org

- **com**: تستخدم بشكل عام للمواقع التجارية والشركات. مثل: Facebook.com

- **net**: تستخدم بشكل أساسي للشركات المرتبطة بالشبكات. مثل: Speedtest.net

- امتدادات دومين المستوى العالي المعنوية (**sTLDs) (Sponsored Top-Level Domains**): هذه الفئة تشمل امتدادات ترتبط بصناعات أو قطاعات معينة.

- **edu**: تستخدم للمؤسسات التعليمية. مثل: Uot.edu.ly - الموقع الرسمي لجامعة طرابلس
- **gov**: تخصص للحكومات والجهات الحكومية. مثل: Gnu.gov.ly - الموقع الرسمي لحكومة الوحدة الوطنية

- امتدادات دومين المستوى العالي الجغرافي (**ccTLDs) (Country code Top-Level Domains**): هذه الامتدادات مرتبطة بدول معينة أو مناطق جغرافية. تُستخدم عادة لمواقع محددة لتلك الدول أو المناطق.

- **ly**: ليبيا. مثل: Annir.ly - الموقع الرسمي لمبادرة أنير الليبية
- **uk**: المملكة المتحدة. مثل: BBC.co.uk - الموقع الرسمي لوكالة الاعلام البريطانية بي بي سي
- **de**: ألمانيا. مثل: Tripolis.diplo.de - الموقع الرسمي للسفارة الألمانية في طرابلس

- **الخلاصة:**

الانتباه لامتداد الدومين الخاص بموقع معين يعتبر خطوة أولية مهمة جداً في التحقق من بيانات المواقع الإلكترونية.

- -على سبيل المثال- يمكن أن نفهم من الامتداد (:Uot.edu.ly)
  - edu: أنه يتبع مؤسسة تعليمية.
  - ly: أن هذه المؤسسة ليبية.

أيضاً، في بعض الأحيان يمكن لامتداد الدومين أن يعطينا نظرة أولية عن موثوقية محتوى موقع معين. - على سبيل المثال- يمكن الاعتماد على المواقع التي تحمل الامتداد ".gov" كمصدر موثوق للمعلومات؛ لأن هذا الامتداد لا يمكن الحصول عليه الا عن طريق المؤسسات الحكومية، على عكس الامتدادات التجارية الأخرى ".com" أو ".net" التي يمكن لأي أحد الحصول عليها.

- **أدوات تقنية:**

يوجد العديد من الأدوات التقنية المساعدة للتحقق من بيانات المواقع الإلكترونية، حيث يمكننا باستخدام هذه الأدوات التحقق من مدى موثوقية الموقع واحتمالية ارتباطه بمواقع أخرى تنشر المعلومات المضللة أو الوصول لبيانات مهمة مثل: معلومات المالك أو الخوادم الخاصة بالموقع ... وغيرها الكثير، التي قد تكون مهمة أثناء عملية التحقق.

4.2. أداة "ScamAdviser" [26] [27]:

تهدف أداة "ScamAdviser" لمساعدة المستخدمين/ات على تقييم مدى موثوقية المواقع على الإنترنت، والتحقق مما إذا كانت مواقع محتملة للاحتيال أم لا. بشكل عام، يتم استخدام هذه الأداة في فحص مواقع التجارة الالكترونية -قبل الشراء منها- للتحقق من مدى موثوقيتها والتأكد من أنها آمنة وحقيقية.

تتميز هذه الأداة بعرضها اللطيف للبيانات وتسهيل قراءتها للعامة، وكذلك بتقديمها تقييم مبدئي لمدى موثوقية الموقع المراد البحث عنه، وذلك بتحليل مجموعة من البيانات لتوليد تصنيف لموقع ويب معين، مع الأخذ بعين الاعتبار مدى اتباع معايير السلامة الرقمية وإجراءات حماية الخصوصية من قبل الموقع المراد البحث عنه.

وعلى الرغم من كون هذا التقييم المبدئي مفيداً في بعض الحالات، إلا أنه يجب استخدامه بحذر ولا يجب الاعتماد عليه بشكل كامل. بمعنى، قد يحصل موقع ينشر الأخبار الخاطئة والمضللة على تقييم 100/100 من قبل الأداة وذلك لاتباعه كافة معايير السلامة الرقمية المتعارف عليها في الفضاء الرقمي. إلا أن هذه المواقع -في العادة- لا تتبع هذه المعايير مما يجعل التقييم المبدئي مفيداً في بعض الأحيان، ولكن ليس للمستوى الذي نعتمد عليه كلياً.

كما توفر الأداة أيضاً إمكانية عرض تحليل مفصل لبيانات الوقع، مما يتيح للمستخدمين/ات إمكانية الاطلاع عليها بشكل يدوي بدون تدخل خوارزميات الأداة.

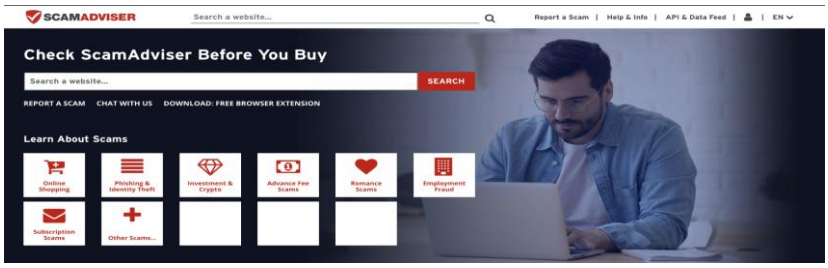
- باستخدام هذه الأداة، يمكن الوصول للعديد من البيانات مثل:

- العمر النسبي للموقع: يقيس مدى مرور وقت على إنشاء الموقع. يُفترض أن المواقع القديمة أكثر موثوقية من المواقع الجديدة.
- مكان الاستضافة: يحلل موقع الاستضافة للموقع، حيث إن المواقع التي تستضيفها خوادم معروفة وموثوق بها قد تكون أكثر أمانًا.
- مالك الموقع وبيانات الاتصال: يحاول تحديد من يمتلك الموقع ومعلومات الاتصال المتاحة. هذا يساعد في تحديد ما إذا كان الموقع يقدم معلومات كافية وشفافية حول هويته.
- التقييمات والشهادات: يبحث عن التقييمات والآراء السلبية والإيجابية حول الموقع على الإنترنت. ومع ذلك، يجب أن يؤخذ في الاعتبار أن بعض المواقع الجيدة قد تكون هدفًا لحملات تشويه منافسين أو تلاعب بالتقييمات.
- وجود عناصر مشبوهة: يحاول الكشف عن عناصر مشبوهة في التصميم أو الهيكل أو روابط البريد الإلكتروني، والتي قد تشير إلى أن الموقع قد يكون مشبوهًا.

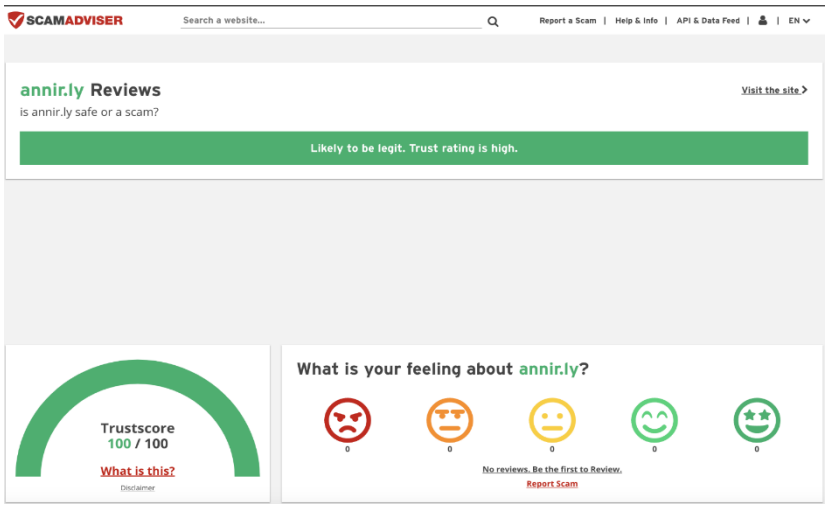
- استخدام أداة "**ScamAdviser**":

- الدخول للموقع الخاص بالأداة.

- وضع رابط الموقع المراد التحقق منه في الحقل الخاص به.



- النقر على زر بحث، وانتظار النتائج.



4.3. أدوات أخرى:

على الرغم من كون "ScamAdviser" تقدم معلومات مفيدة، فإنها ليست مثالية وقد تكون هناك حالات خاصة تختلف فيها النتائج. من الضروري دائماً مراجعة المعلومات بعناية واستخدام مصادر أخرى للتحقق. في الحقيقة توصي ScamAdviser نفسها بعدم الاعتماد على تصنيفاتها فقط وبدلاً من ذلك دعمها بالبحث والتحقق الشخصي.

4.3.1. Whosiology
4.3.2. Who.is
4.3.3. ICANN Lookup

5. التحقق من حسابات وسائل التواصل الاجتماعي "Social Media"

أثناء التحقق من المعلومات أو الأخبار، قد تتطلب بعض القضايا التحقق من مرجعية أو ملكية الحسابات على وسائل التواصل الاجتماعي؛ وذلك بسبب سهولة انتحال الهوية للأفراد أو المؤسسات على هذه المواقع وإنشاء صفحات مزيفة بأسمائهم.

- **هل علامة التوثيق تعني الموثوقية؟**

الاجابة القصيرة هي لا. علامة التوثيق لا تعنى أن الصفحة المعنية تنشر أخباراً صحيحة أو موثوقة، وإنما هي في الواقع تشير الى ان هذا الحساب -فرد كان أو مؤسسة- قد استوفى شروط التوثيق الخاصة بالمنصة من تقديم مستندات شخصية تثبت هوية مالك الحساب وأن المنصة بدورها قد تحققت من هويتهم.

على سبيل المثال، إذا قامت المؤسسة (أ) بتوثيق حساباتها على مواقع التواصل الاجتماعي، هذا يعني بأن هذا الحساب الموثق هو الحساب الرسمي والصحيح للمؤسسة (أ) وكل الحسابات الأخرى التي تحمل نفس الاسم هي حسابات مزيفة. ولكن هذا لا يعني أن الأخبار التي تنشرها هذه المؤسسة لا يمكن أن تكون خاطئة أو مضللة.

- **منصات التواصل الاجتماعي والتوثيق**

تختلف شروط التوثيق من منصة تواصل اجتماعي إلى أخرى. حيث تعتمد بعض المنصات على وجود علامة توثيق واحدة تشمل كل التصنيفات، بينما تعتمد بعض المنصات الأخرى على أكثر من علامة للإشارة لتصنيف الفرد أو المؤسسة مثل: (جهات حكومية، شخصيات عامة، شركات خاصة، توثيق مدفوع).

- ما فائدة علامة التوثيق للمستخدمين/ات؟

مثلما ذكرنا سابقاً، فالحسابات الموثقة تعني حقيقة هوية مالك/ة الحساب ولا ترتبط بصحة المعلومات التي يتم نشرها عليه. ولكن في بعض الحالات، يمكننا الاستفادة من هذا التوثيق في سياق التصريحات الرسمية للمؤسسات الحكومية أو الجهات العامة أو الخاصة.

ولكن من أجل الاستفادة الكاملة وعدم الوقوع ضحية عدم الدراية، يجب على المستخدمين/ات أو مدققي/ات المعلومات إدراك وفهم معايير التوثيق المختلفة بكل منصة، لا سيما في إطار إطلاق اشتراكات توثيق مدفوعة.

5.1. الحسابات الموثقة على فيسبوك وانستاجرام

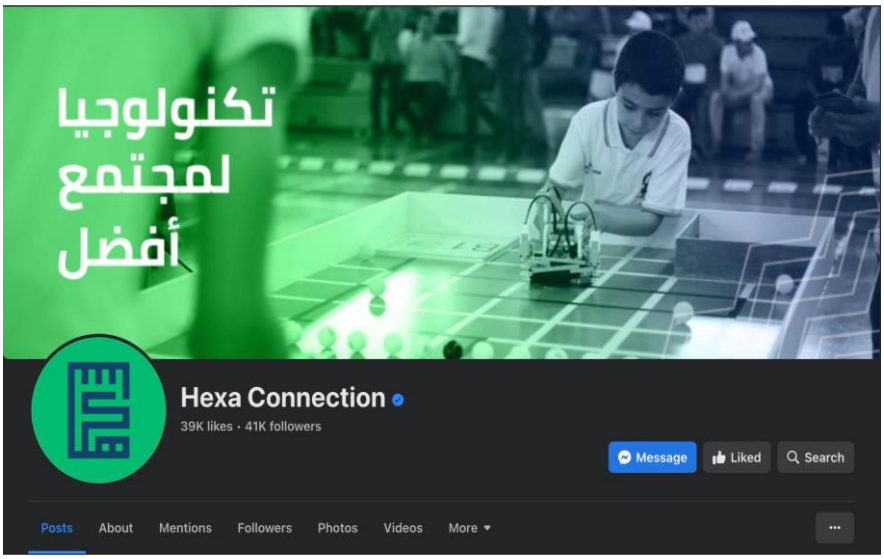
تعتمد منصتا فيسبوك وانستاجرام التابعتين لشركة ميتا "Meta" على علامة واحدة للتوثيق وهي العلامة الزرقاء . في السابق، اشترطت ميتا ضرورة كون المستفيد شخصية عامة، أو مشهورة، أو مؤسسة معروفة، أو علامة تجارية عالمية بغرض الحصول عليها ضمن برنامج العلامات الموثقة الخاصة بها "Verified Badge". والجدير بالذكر أن هذا البرنامج يتيح الحصول على علامات التوثيق للأفراد على حساباتهم الشخصية "Profiles" أو على الصفحات العامة "Pages". [28]

إلا أنه مؤخراً -في الربع الأول من عام 2023- تم إطلاق برنامج آخر للتوثيق يسمى برنامج ميتا للعلامات الموثقة "Meta Verified Badge" متاح للأفراد عبر حساباتهم الشخصية "Profiles" فقط، وهي خدمة مدفوعة باشتراك شهري متاحة للجميع ولا يشترط فيها كون المستفيد/ة شخصية مشهورة أو عامة، فبمجرد تقديم المستخدم/ة المستندات والقيمة الشهرية المطلوبة وموافقة المنصة على طلبه، سيتحصل على ميزات هذا البرنامج والتي تشمل علامة التوثيق الزرقاء والعديد من الميزات الأخرى مثل: (الأولوية في الدعم الفني، وملصقات خاصة داخل المنصة، وغيرها). [29]

وهكذا، يمكن أن نفهم أن الحسابات الموثقة على منصة فيسبوك تعبر عن هوية الأشخاص أو المؤسسات التي تدير هذه الحسابات، ويمكن الاعتماد عليها في اقتباس التصريحات والأقوال كونها "الحسابات الرسمية".

- **ملاحظة:**

الجدير بالذكر أن البرنامج الأول الخاص بالتوثيق "Verified Badge" لا يزال متاحاً حتى الآن للأفراد والمؤسسات الذين يستوفون شروط المنصة -الشخصيات العامة والمؤسسات بدون مقابل مادي-، بينما يقتصر عمل البرنامج الثاني "Meta Verified Badge" على الأفراد الراغبين في التوثيق فقط بمقابل مادي شهري.



(مثال: صفحة منظمة "Hexa Connection" على فيسبوك موثقة بالعلامة الزرقاء ضمن البرنامج الأول "Verified Badge" الخاص بتوثيق الصفحات العامة "Page" والمشهورة.)

الحسابات الموثقة على تويتر "X" [11]

اعتمدت منصة " "X(تويتر سابقاً) على علامة واحدة للتوثيق وهي العلامة الزرقاء ، تم إعطاء هذه العلامة للحسابات الرسمية والنشطة والبارزة مثل المشاهير والإعلاميين/ات والسياسيين/ات والمؤسسات

المختلفة والتي يتم التحقق منها من قبل فريق تويتر بشكل مستقل قبل منح ميزة التوثيق، بناء على آلية وإجراءات معينة يتم اتباعها وفقاً لسياسة الشركة بالخصوص. ويشار لها حالياً تحت اسم " Twitter Legacy Verification". [30]

ولكن مع كل التغييرات الجديدة في المنصة خلال عام 2023، تغيرت معايير التوثيق بإطلاق خدمة تسمى تويتر بلو "Twitter Blue - X Premium" مع اعتماد علامات توثيق جديدة.

- **"Twitter Blue - X Premium":**

تويتر بلو، هي خدمة توثيق جديدة مقدمة من منصة تويتر. تتيح هذه الخدمة توثيق الحسابات مقابل اشتراك شهري واستيفاء بعض الشروط البسيطة المشار لها في سياسات الخدمة الخاصة بالمنصة. ابتداء من 1 أبريل 2023، بدأت تويتر بتغيير معايير التوثيق القديمة وإيقاف قبول الطلبات وإغلاق البرنامج، واشترطت دفع قيمة شهرية للحسابات الراغبة في الحصول على علامة التوثيق، أو الحسابات التي حصلت عليها بالفعل ضمن البرنامج القديم "Twitter Legacy Verification" للحفاظ عليها. [31]

- علامات التوثيق الجديدة:

لتفادي التضليل ومحاولات النصب والاحتيال المحتملة بعد إطلاق خدمة تويتر بلو، أطلقت المنصة أربع علامات توثيق مع وضع توضيح لكل واحدة منها.

5.1.1. علامة التوثيق الزرقاء :

تظهر علامة التوثيق الزرقاء أمام نوعين من الحسابات على تويتر:

- الحسابات الموثقة ضمن الآلية القديمة **"Twitter Legacy Verification"**

تظهر علامة التوثيق الزرقاء بجانب أسماء الأفراد الموثقة حساباتهم بالمعايير القديمة "ناشط، وبارز، وأصلي" وقبل إطلاق خدمة التوثيق الجديدة "تويتر بلو". اشترطت المنصة على من يحصل

على علامة التوثيق ضمن الشروط القديمة دفع مقابل شهري لإبقاء علامة التوثيق، ولكن بدون الخوض في إجراءات التأكد من هوية صاحب الحساب لأن هذا الأمر قد تم بالفعل ضمن المعايير القديمة.

يمكن معرفة هذه الحسابات عند الضغط على علامة التوثيق وتفقد تاريخ الحصول على علامة التوثيق -قبل 1 أبريل 2023- وذلك للتفرقة بين الحسابات الموثقة ضمن الآلية القديمة وبين الحاصلين على العلامة ضمن البرنامج الجديد.

(مثال لحساب الكاتبة البريطانية J.K Rowling على "X" والحاصلة على علامة التوثيق الزرقاء منذ 2009)

- الحسابات الموثقة ضمن الآلية الجديدة **"Twitter Blue - X Premium"**

تظهر علامة التوثيق الزرقاء بجانب الحسابات الموثقة بمقابل مادي ضمن خدمة تويتر بلو، وذلك بعد استيفاء شروط الحصول عليها، ويمكن تفرقة الحسابات الخاصة بأفراد عاديين بتفقد تاريخ الحصول على علامة التوثيق.

(مثال لحساب فرد على "X" والحاصل على علامة التوثيق بعد إطلاق الخدمة الجديدة "X Premium")

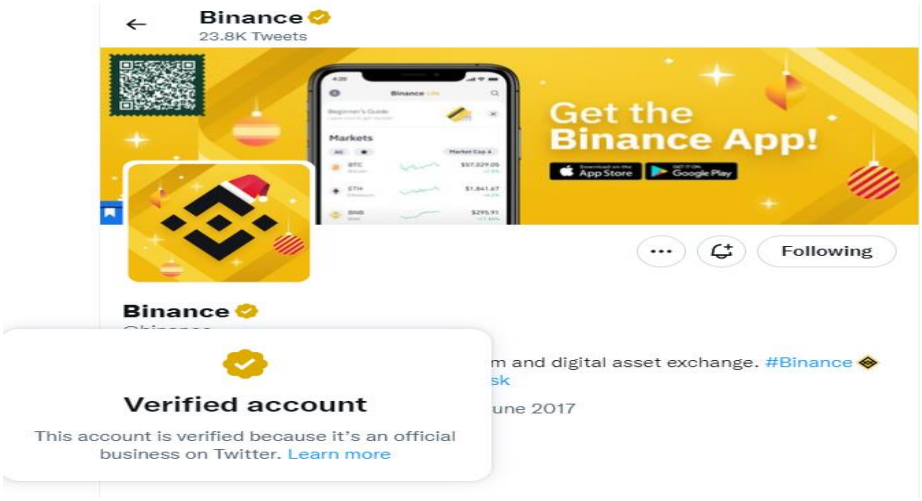
5.1.2. علامة التوثيق الرمادية

التي تظهر بجانب حسابات الأفراد أو المؤسسات ذات الصلة بالحكومات، ويشار لهم عند الضغط على علامة التوثيق بـ" Verified because it is a government or multilateral organization".

(مثال لحساب البيت الأبيض على "X" والحاصل على علامة التوثيق الرمادية الخاصة بالمؤسسات الحكومية)

5.1.3. علامة التوثيق الذهبية

التي تظهر بجانب حسابات الشركات أو مشاريع القطاع الخاص، ويشار لهم عند الضغط على علامة التوثيق بـ"Verified because it's an official business".



(مثال لحساب منصة Binance لتداول العملات الرقمية على "X" والحاصل على علامة التوثيق الذهبية الخاصة بالشركات)

- **تسهيل تمييز علامات التوثيق**

مع تغيير سياسات التوثيق الخاصة بمنصة تويتر وإضافة العديد من علامات التوثيق، أصبح تمييز الحسابات الرسمية أمراً معقداً خاصة عند ظهور التغريدات في الصفحة الرئيسية. يمكن استخدام بعض الطرق أو الأدوات الرقمية لتمييز حقيقة هذه الحسابات.

- **الفحص اليدوي للحسابات:**

وذلك عبر الدخول لصفحة الحساب والضغط على علامة التوثيق وقراءة الوصف الخاص بها والتحقق من تاريخ الحصول على علامة التوثيق.

- **إضافة "Eight Dollars":**

وهي إضافة على المتصفحات تسهل تمييز الحسابات الموثقة من بعضها البعض، وذلك عبر إظهار:

- كلمة موثق "**Verified**" أمام كل الحسابات الموثوقة:
  - Blue: Legacy
  - Blue: notable
  - Golden: Business
  - Grey: Government

- كلمة "**Paid**" أمام الحسابات المشتركة في خدمة التوثيق:
  - Blue - subscribed

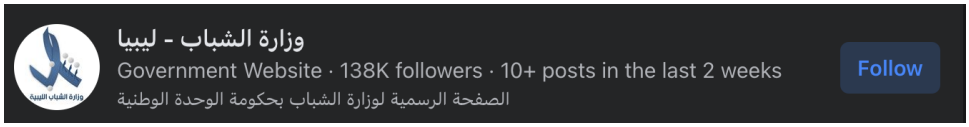
5.2. صفحات رسمية غير موثقة

توجد العديد من الحسابات والصفحات التي تعود إلى جهات دولية، أو حكومية، أو رسمية، أو إلى شخصيات عامة قد لا تمتلك علامة التوثيق لسبب أو لآخر. ربما بسبب أن بعضها لم يقدم طلباً للحصول على علامة التوثيق، أو أنها تفتقر للمعايير المطلوبة للحصول على العلامة.

- وبذلك يجب على المستخدم التأكد من تبعية الحساب عن طريق اعتماد طرق أخرى مثل:
- تفقد الموقع الرسمي الخاص بالمؤسسة -يتم مراعاة طرق التأكد من موثوقية مواقع الويب المذكورة سابقاً-.
- تفقد معايير شفافية الصفحة على منصة فيسبوك.

- على سبيل المثال:

لا تمتلك صفحة "وزارة الشباب - ليبيا" علامة التحقق الخاصة بفيسبوك، ولكن مع ذلك تعتبر الصفحة الرسمية والمعتمدة لوزارة الشباب والرياضة.



- فكيف نثبت حقيقة تبعيتها للوزارة؟

5.2.1. البحث عن الموقع الرسمي الخاص بالوزارة عبر محركات البحث:

نستخدم عند البحث كلمات مفتاحية مثل: "وزارة الشباب في ليبيا"، وبالنظر الى نتائج البحث نستطيع تحديد موقع يدعي بأنه الموقع الرسمي الخاص بوزارة الشباب تحت الرابط: Youth.Gov.Ly.

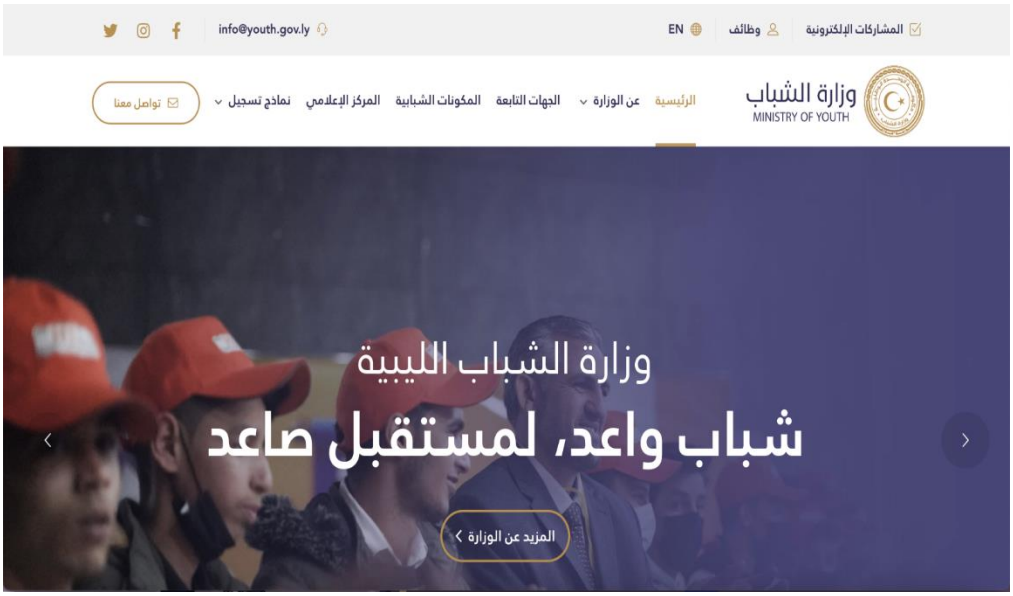
ومن الوهلة الأولى يمكن ملاحظة أن رابط الموقع يحمل امتداد نطاق ".Gov" الذي تمتلكه الجهات الحكومية فقط. ويحمل الرابط كذلك امتداد ".Ly" وهو امتداد للمواقع التي تنتمي لليبيا. وبذلك نستنتج أن الموقع " Youth.Gov.Ly" ينتمي لجهة حكومية في ليبيا.

5.2.2. تحليل بيانات الموقع:

باستخدام أداة ScamAdviserنقوم بلصق رابط الموقع الذي تحصلنا عليه من نتائج محرك البحث، ومن ثم التحقق من هوية مالك الموقع وتسجيل المؤسسة والخوادم المستضاف عليها. يمكن في هذا المثال تخطي هذه الخطوة لأنه تم بالفعل إثبات أصالة الموقع عن طريق امتداد الدومين، ولكنها ستكون ذات فائدة أكبر في حال كون الموقع يتبع مؤسسة غير حكومية.

5.2.3. زيارة الموقع:

بعد زيارة الموقع يمكننا ملاحظة أيقونات مواقع التواصل الاجتماعي أعلى يسار الموقع، وعند الضغط على أيقونة الفيسبوك ستظهر صفحة الفيسبوك الخاصة بالوزارة وهي غير موثقة بالعلامة الزرقاء، ولكنها تعتبر الصفحة الرسمية نظراً لتواجدها في موقعهم الرسمي.



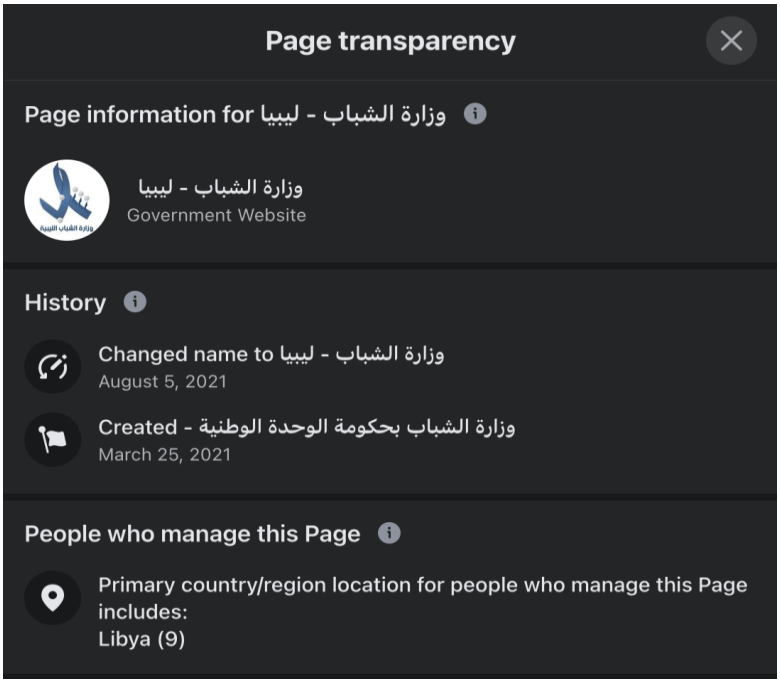
وبهذه الطريقة تأكدنا بأن صفحة الفيسبوك الموجودة على هذا الرابط -غير الموثقة- هي فعلاً صفحة رسمية تتبع وزارة الشباب في ليبيا.

5.2.4. معايير شفافية الفيسبوك [27]

يمكن للمستخدم أيضاً تسخير معايير الشفافية الخاصة بفيسبوك لصالحه ولإثبات موثوقية الصفحات على هذه المنصة.

- يمكن الوصول لبيانات الشفافية الخاصة بصفحة معينة على فيسبوك عن طريق:
  - الدخول إلى الصفحة المطلوبة.
  - النقر على قسم "عن" "About".
  - من ثم "شفافية الصفحة" "Page transparensy".

وبتطبيق هذه الخطوات على المثال السابق، يمكننا الاطلاع على شفافية صفحة وزارة الشباب على فيسبوك.



- عن طريق هذه البيانات يمكن أن نستفيد من:

- سجل تغيير اسم الصفحة

في حال كانت الصفحة مريبة أو غير رسمية، قد نلاحظ تغيير اسمها مراراً وتكراراً في سياقات مختلفة ومتباعدة.

- **الموقع الجغرافي وعدد مدراء الصفحة:**

في حال كانت الصفحة مريبة أو غير رسمية أو تصيدية وتنتحل هوية مؤسسة معينة، قد نلاحظ كثرة عدد مدراء الصفحة مع اختلاف الموقع الجغرافي لهم/ن عن البلد المستهدفة. فمن غير المنطقي أن تكون صفحة مؤسسة حكومية تدار من قبل أشخاص غير موجودين في ليبيا بتاتاً -على سبيل المثال-.

5.3 "LinkedIn"

منصة "LinkedIn" هي شبكة اجتماعية مهنية تهدف إلى ربط المحترفين/ات في المهن المختلفة وبناء علاقات مهنية. يمكن استخدام هذه المنصة في البحث والتأكد من هويات الأفراد أو الشركات والتحقق من طبيعة عملها.

5.4 "WebMii"

منصة "WebMii" هي عبارة عن أداة لتجميع المعلومات من مصادر مختلفة على الإنترنت. تهدف المنصة إلى عرض معلومات عامة ومتاحة على الإنترنت عن شخص معين في مكان واحد، مما يتيح للمستخدمين/ات فهم الصورة العامة عن هذا الشخص. يمكن استخدام هذه المنصة للبحث عن هوية الأفراد وطبيعة عملهم ونشاطاتهم، وللاستقصاء عنهم واستكشاف المزيد من المعلومات المتاحة على الإنترنت بخصوصهم.

6. خدمات أرشفة المواقع

الأرشفة وأدواتها هي طرق تستخدم لحفظ صفحات الويب بشكل أوتوماتيكي أو يدوي، أو للوصول لنسخ سابقة وقديمة لموقع إلكتروني معين. يتم الاحتفاظ بهذه النسخ المؤرشفة على شبكة الإنترنت حتى بعد حذف الصفحة أو الموقع من على الشبكة.

- **ما هي فوائد الأرشفة؟**

يمكن الاستفادة من "أرشفة المواقع" بعدة أمور، أهمها:

- الوصول إلى معلومات، ومقالات، وأخبار لم تعد موجودة على الإنترنت بسبب أن الموقع لم يعد متاحاً على شبكة الإنترنت (لأسباب تقنية، أو مادية، أو إدارية).
- الوصول إلى معلومات، ومقالات، وأخبار لم تعد موجودة على الإنترنت بسبب حذف الموقع للمادة أو الخبر.
- الوصول إلى معلومات، ومقالات، وأخبار غيّر أحد المواقع محتواها أو عدّل عليه.
- حفظ الروابط من الضياع؛ والتي من الممكن أن تستخدم لاحقاً كمصادر أو مراجع.

- لماذا يعتبر استخدام الأرشفة مهماً؟

في بعض الأحيان، نعتمد في حياتنا اليومية على أخذ لقطات شاشة كإثبات وجود محتوى معين في وقت معين على صفحات مواقع التواصل الاجتماعي أو مواقع الإنترنت، أو حفظ الصفحة المرادة كـPDF لاستخدامها لاحقاً كمصدر أو دليل لقضية معينة.

في سياق الحياة اليومية، قد تكون هذه الطرق مفيدة. ولكن عندما نتكلم عن طرق العمل الاحترافي أو إثبات موثوقية أو أصالة محتوى معين، قد لا تكون الطرق السابقة أفضل خيار، وذلك لعدة أسباب منها:

- سهولة تزوير لقطات الشاشة.
- إمكانية التعديل أو تزوير صفحات الويب بعد حفظها كـPDF.

ولهذه الأسباب، لا يعتد بالطرق المذكورة سابقاً كدليل أو مصدر أو كإثباتات لتواجد محتوى معين على الإنترنت في سياق تدقيق المعلومات.

- **ما الحل؟**

هنا تكمن قوة أدوات الأرشفة، إذ تعتبر كطرف ثالث مفتوح المصدر يقوم بالدخول إلى الصفحات المراد حفظها، ويخزنها على الخوادم الخاصة به. وبهذه الطريقة لا يكون المستخدمون/ات هم/ن من يقدمون الدليل. باستخدام أدوات الأرشفة يطلب المستخدم/ة من موقع الأرشفة الدخول على الصفحة المرادة وتخزينها، وبدوره سيقوم الموقع بالدخول إلى الصفحة وأخذ لقطة كاملة لها وحفظها بكل الروابط. ولكون هذه الأدوات مفتوحة المصدر، لا يتم التشكيك في مصداقيتها وذلك بسبب كون الكود البرمجي الخاص بها مفتوح للعامة ويمكن للجميع أن يرى كيفية عمله، وهي تقتصر فقط على الدخول إلى الصفحة المرادة وتخزينها. ولهذا السبب يمكن الاعتماد على الصفحات المؤرشفة كدليل لوجود محتوى معين على صفحات الإنترنت بشكل موثوق.

6.1. أداة العودة بالزمن ""Wayback Machine"

في بعض الأحيان يحتاج المستخدمون/ات للرجوع إلى نسخ قديمة من صفحات موقع إلكتروني معين، وذلك لعدة أسباب تشمل تعطل الموقع أو تغير محتواه أو حذف صفحاته تماماً. وكما يوحي الاسم، توفر أداة العودة بالزمن "Wayback Machine" خدمة أرشفة صفحات المواقع، والتي تمكن المستخدمين/ات من البحث عن نسخ مؤرشفة سابقاً لصفحات ومحتوى المواقع.

تتميز هذه الأداة بأرشفتها لصفحات الويب على الإنترنت السطحي بشكل أوتوماتيكي -في حالة سماح الموقع الالكتروني بذلك-. بشكل دوري، تقوم عناكب هذه الأداة بالزحف على صفحات الويب وأخذ لقطات شاشة لها وحفظها في قاعدة بيانات الأداة. تتاح هذه اللقطات للمستخدمين/ات في حالة بحثهم/ن عن نسخة سابقة من موقع معين أو للاطلاع على محتوى موقع معين بعد حذفه.

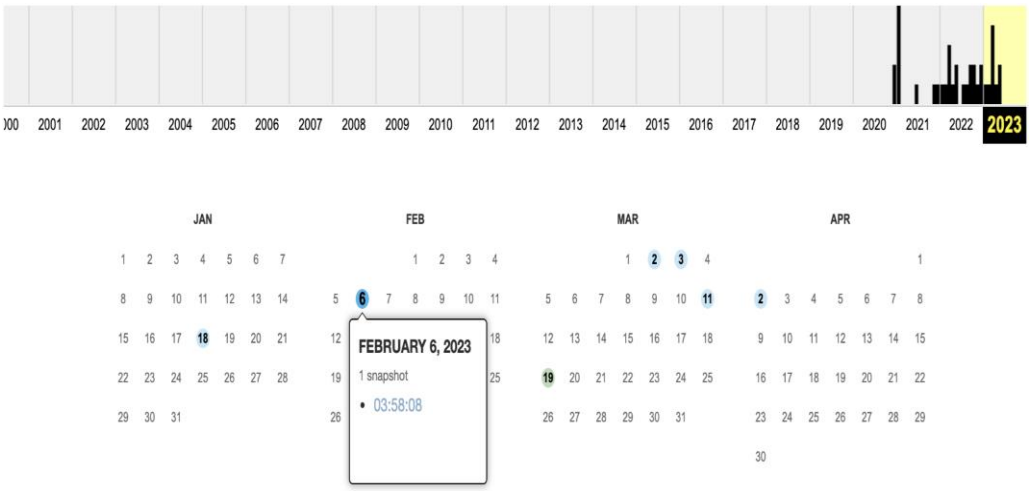
أيضاً، تقدم هذه الأداة خدمة الأرشفة بشكل يدوي، وذلك بإدخال رابط الصفحة المراد أرشفتها -منشور على فيسبوك على سبيل المثال- وستقوم الأداة بالدخول إلى الصفحة وأرشفتها، وبعد ذلك يمكن استخدامها كدليل موثوق.

6.1.1. طريقة البحث عن نسخ مؤرشفة سابقاً:

- من خانة البحث داخل الأداة يمكن إدخال رابط الموقع المراد البحث عن نسخ مؤرشفة منه، في هذه الحالة ندخل موقع أنير على سبيل المثال.
- نضغط على زر "إدخال" أو "Enter".
- عندها ستظهر لنا نتيجة البحث والنسخ المؤرشفة من الموقع خلال الأشهر والسنوات الماضية في حال توفرت.

في المثال الحالي، عند البحث عن نسخ مؤرشفة لموقع "أنير" (Annir.ly), سيظهر عدد من النسخ المؤرشفة للموقع خلال السنوات 2020, 2021, 2022, 2023.

يمكن الوصول إلى أي من النسخ المؤرشفة عبر تحديد السنة من الشريط العلوي، ثم نحدد الشهر واليوم كما يظهر في الصورة التالية:



- ملاحظة:

- يشير اللون الأزرق والأخضر الموجود على التقويم إلى توفر نسخ مؤرشفة للموقع في هذا اليوم.
- يشير حجم الدائرة إلى عدد النسخ المتوفرة في هذا اليوم؛ كلما كبرت الدائرة، كان عدد النسخ أكثر.

6.1.2. طريقة أرشفة منشور أو تغريدة للعودة لها لاحقاً أو لاستخدامها كمرجع:

- الدخول على الصفحة الخاصة بالحفظ على موقع "Wayback Machine".

- وضع رابط المقال، أو المنشور، أو التغريدة في حقل "Save Page Now".

- الضغط على خيار "Save Page".

الخاتمة

عزيزي القارئ، عزيزتي القارئة،

بعد انتهائنا معًا من قراءة هذا الدليل، مرورًا بأقسامه ومحطاته المختلفة. ها نحن نقف على عتبة الختام. خلال هذه الرحلة المثيرة، تمكنا بلا شك من تجسيد فهمٍ شامل لاضطراب المعلومات وتأثيراته التي تمتد إلى أعماق المجتمع. تعرّفنا أيضًا على الدور الحيوي الذي يلعبه تدقيق المعلومات في مواجهة اضراب المعلومات، كما

تعلمنا الطرق السليمة للتفكير واستخدام أشهر الأدوات في عمليات التحقق من المحتوى الرقمي وكيفية تسخيرها للوصول إلى الحقيقة.

- **أخيراً، نضع بعين الاعتبار:**

  - **التحقق من المعلومات ليس بالأمر السهل**

بالرغم من توفر العديد من وسائل التحقق من المعلومات، ينبغي لنا أن ندرك أن نتائج البحث قد تكون مقيدة في بعض الأحيان. حيث تعتمد هذه النتائج على المصادر المُتاحة على الإنترنت أو على قواعد بيانات الأدوات المستخدمة، مما قد يؤدي إلى نتائج غير دقيقة، أو حتى تقديم معلومات غير مرتبطة بالسياق المطلوب. يجب أن ندرك أيضًا أن تدقيق المعلومات هو عملية تعتمد على تنوع المنهجيات والأدوات. حتى عند صياغة الأسئلة الملائمة واستخدام الأدوات المناسبة، قد نجد أحيانًا أن الطريق مسدود والإجابات غير واضحة.

  - **أدلة أكثر، مصداقية أكثر**

يتجلى تدقيق المعلومات كعملية تتسم بالتعقيد والبساطة في الوقت ذاته. أحيانًا، يمكننا اكتشاف الحقيقة منذ بداية عمليات التحقق، وفي بعض الأحيان قد تأخذ عملية التحقق ساعات أو حتى أيام من البحث والتحري. على كل حال، بالصبر وتحري الدقة يمكننا جمع الأدلة من مصادر متعددة وربطها ببعضها، واستخدام العديد من الأدوات التنقية في نفس الموضوع، مما يمنحنا دليلًا قويًا في النهاية.

بعبارات أبسط، لحل الأحجية يجب علينا تجميع كل الأجزاء المفقودة، ويتم ذلك بربط مهاراتنا في التفكير والتحليل والنظر ما وراء الخبر أو المعلومة واستعمال مختلف أدوات التحقق حتى عند الوصول إلى نتيجة مرضية، وذلك لضمان الحصول على أكثر من دليل قاطع يدعم نفس الإجابة.

- **مسؤوليتنا جميعاً: إنترنت أكثر أماناً**

في عصرٍ أصبحت فيه المعلومات المضللة صناعة احترافية، أصبحت عملية التحقق ضرورية للحفاظ على دقة المعلومات ومصداقيتها. ومع نشر الوعي الإعلامي وتعميم ثقافة تدقيق المعلومات، يمكننا جميعاً كمستخدمين/ان ومدققي/ات معلومات أن نساهم في جعل الإنترنت مكاناً أكثر أمانًا.

- **إخلاء طرف:**

مبادرة أنير غير ملزمة بأي تغيير في المعلومات المذكورة في هذا الدليل بعد موعد نشره وحتى إصدار نسخة جديدة منه. المعلومات المذكورة في هذا الدليل تمت كتابتها استناداً على مصادر موثوقة. بعد نشر هذا الدليل، قد تتغير بعض المعلومات القابلة للتطوير مثل سياسات منصات مواقع التواصل الاجتماعي.

- تجدون في الهوامش روابط لأمثلة متوسعة تقدم تفاصيل وتوضيحات إضافية حول المفاهيم والاستراتيجيات المطروحة.

- الهوامش:

[1]: يونسكو - مكافحة الأخبار الزائفة

[2]: أنير - الذباب الإلكتروني: كيف يؤثّر علينا؟

[3]: أنير - أنير تعثر على شبكة ذباب إلكتروني على تويتر

[4]: يوتيوب - مواجهة اضطراب المعلومات في ليبيا: دور تدقيق الحقائق والأدوات التقنية

[5]: أنير - من وين تجي الأخبار الزائفة؟

[6]: أنير - علاش نصدقوا في الأخبار الزائفة؟

[7]: أنير - بروباغاندا الأدمن: كيف تؤثّر المنشورات والميمز في المشهد السياسي؟

[8]: أنير - التأطير في الأخبار

[9]: أنير - ست طرق تساعدكم على تمييز الأخبار الزائفة

[10]: أنير - سيكولوجية تدقيق الحقائق

[11]: أنير - طرق تدقيق الحقائق وانعكاسات تطور الساحة الرقمية

[12]: "FullFacts" - دليل "FullFacts" للتحقق من المعلومات

[13]: أنير - مضلل: هذه الصورة ليست للخطوط الجوية الليبية

[14]: أنير - مضلل : لم يقم هذا الشخص بحرق دفتر ديون الزبائن بمناسبة شهر رمضان في ليبيا

[15]: أنير - مضلل: هذه الإشارة احترقت في مدينة ميلانو وليست في منطقة العزيزية

[16]: أنير - مضلل: هذه الصورة لمنظومات اضاءة صحراوية ليست في ليبيا، بل في السعودية

[17]: أنير - زائف: لم تنجب هذه السيدة من جنوب أفريقيا 11 طفلاً

[18]: أنير - زائف: هذه الصورة ليست لمطار طرابلس الدولي بل لمطار في مالدوفا

[19]: أنير - مضلل: هذه الفتاة التي تساعد والدها الميكانيكي ليست ليبية

[20]: أنير - ظهور فِيَلَة في الجنوب الليبي

[21]: أنير - مضلل : مقطع قتل 7 أطباء تخدير في مزرعة صديقهم قديم وسياقه مختلف

[22]: أنير - مضلل: هذا الفيديو لامرأة محجبة تقود سيارة مكشوفة ليس في ليبيا

[23]: أنير - زائف: هذا الفيديو لمشجارة بين شاب وفتاة في العراق وليس في ليبيا

[24]: أنير - زائف: لم يتم وضع هذا التمثال مكان تمثال الغزالة سابقاً

[25]: أنير - مضلل: لم تبدأ الأنهار بالظهور في صحراء المملكة العربية السعودية.

[26]: أنير - تدارك أخطاء الماضي: نتائج الشهادتين الإعدادية والثانوية في ليبيا

[27]: أنير - ما حقيقة اكتشاف الطالبة الليبية عائشة المنصوري علاجا للروماتيزم؟

[28]: فيسبوك - طلب الحصول على شارة مُحقّقة على فيسبوك

[29]: فيسبوك - حول ميزة Meta Verified على فيسبوك

[30]: تويتر "X" - سياسة التوثيق القديمة

[31]: تويتر "X" - كيفية الحصول على علامة الاختيار الزرقاء على Twitter

[32]: أنير - من نحن

عن أنير[32]

أنير هي مبادرة ليبية مستقلة، محايدة وغير سياسية، مختصة في التوعية بشؤون الإنترنت الآمن والتحقق من الأخبار الزائفة والمعلومات المضللة. نشأت عام 2020، وتتخذ من الفضاء الإلكتروني منصة لها تهدف إلى رفع الوعي بالممارسات السليمة لخوض تجربة إنترنت أكثر أمانا.

تقوم أنير بنشر محتوى توعوي حول السلامة والحقوق الرقمية والتكنولوجيا، كما تكافح اضطراب المعلومات وذلك عبر التوعية بشؤون التربية الإعلامية والمعلوماتية، والتحقق من الأخبار الزائفة والمضللة المنتشرة عبر وسائل التواصل الاجتماعي.

سياسة استخدام دليل أنير للتحقق من المحتوى الرقمي

مشروع قانون الجرائم الافتراضية والدليل الرقمي

مشروع قانون الجرائم الافتراضية والدليل الرقمي

إن اصدار القانون رقم (05) لسنة 2022 بشأن مكافحة الجرائم الالكترونية لم يأتي فجأة.. بل سبقته العديد من المبادرات والمطالبات للجهات المسئولة بشأن أهمية وضرورة اصدار قانون للجرائم الافتراضية ولعل أولى هذه المبادرات المقترح الذي تقدمت به موسوعة التشريعات العربية سنة 2008 لأمانة اللجنة الشعبية العامة للعدل (سابقا) تحت اسم (مشروع قانون الجرائم الافتراضية والدليل الرقمي) والذي أعيد تقديمه للحكومة من خلال جهاز المباحث الجنائية ووزارة الداخلية. إلا أن هذا المشروع لم يرى النور ولم يأخذ طريقه الى قبة البرلمان. وفيما يلي نعرض لكم من التوثيق النسخة الأولى من هذا المشروع.

اسرة التحرير

مقترح موسوعة التشريعات العربية
لمشروع قانون الجرائم الافتراضية والدليل الرقمي

مشروع القانون رقم..... لسنة..... بشأن الجرائم الافتراضية والدليل الرقمي.

مشروع قانون الجرائم الافتراضية والدليل الرقمي

قانون الاصدار.

الباب الأول: أحكام عامة

الفصل الأول : مبدأ الشرعية الجنائية والامنية

الفصل الثاني : علم الاجرام الافتراضي

الفصل الثالث : سلطة القاضي في تقدير العقوبة

الباب الثاني: القاعدة الموضوعية

الفصل الأول : المصلحة الاجتماعية الاقتصادية

الفصل الثاني : أنواع الجرائم

الفصل الثالث : المسئولية الجنائية

الفصل الرابع : العقوبات الرقمية (التنفيذ)

الباب الثالث: القاعدة الاجرائية

الفصل الأول : الاختصاص القضائي

الفصل الثاني : الاثبات الرقمي

الفصل الثالث : الخبرة التقنية

الفصل الرابع : الارشاد الرقمي

مشروع قانون الجريمة الافتراضية والدليل الرقمي

البرلمان الليبي
بعد الاطلاع على:
الاعلان الدستوري لثورة فبراير المؤرخ / / 2011
وقانون العقوبات.
وقانون الاجراءات الجنائية.
والقانون المدني.
والقانون التجاري.
وقانون المرافعات المدنية.
والقانون رقم لسنة بشأن اعادة تنظيم المحكمة العليا.
والقانون رقم لسنة بشأن الأحوال المدنية ولائحته التنفيذية.
والقانون رقم لسنة بشأن المخدرات والمؤثرات العقلية.
والقانون رقم 9 لسنة 1968 بشأن حماية حق المؤلف.
والقانون رقم 76 لسنة 1972 بشأن المطبوعات.
والقانون رقم 5 لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق.
والقانون رقم..... لسنة..... بشأن مكافحة غسل الأموال.
والقانون رقم 1 لسنة 2005 بشأن المصارف.
والقانون رقم 10 لسنة 1984 بشأن الزواج والطلاق.

أصدر القانون التالي

المادة الاولى
يعمل بقانون الجريمة الافتراضية المرافق دون غيره في إطار الجرائم التي ترتكب بالبدائل المتوافرة حين استخدام الحوسبة والرقمية وكذلك قواعد الاثبات والدليل الرقمي المرفقة به.

المادة الثانية
تشكل بقرار من مجلس الوزراء لجنة من ذوي الاختصاص ذات ميزانية مستقلة لمراقبة تنفيذ هذا القانون ومتابعة تطويره ورصد الدراسات المتعلقة به واعداد التقارير المستمرة حوله وتحضير المذكرات الايضاحية للتعديلات اللاحقة.

المادة الثالثة
يصدر مجلس الوزراء ترشيحا بمن يسمى مأمور ضبط قضائي في اطار تنفيذ هذا القانون بعد استشارة اللجنة المذكورة في المادة الثانية من قانون الاصدار هذا.

المادة الرابعة
يصدر الوزراء، كل في مجال اختصاصه، القرارات المنفذة لهذا القانون بناء على توصية اللجنة المذكورة في المادة الثانية من هذا القانون.

المادة الخامسة
ينشر هذا القانون في الجريدة الرسمية ويعمل به بعد ثلاثة شهور من تاريخ نشرة.
البرلمان الليبي

مشروع قانون الجريمة الافتراضية والدليل الرقمي

الباب الأول
أحكام عامة

الفصل الأول
مبدأ الشرعية الجنائية والأمنية

مادة (1)
مبدأ الشرعية

لا جريمة ولا عقوبة ولا إجراء جنائي ولا تدبير وقائي سابق او لاحق إلا بقانون.

مادة (2)
قواعد أساسية في التفسير

- الرقمية منهج.
- تعد المذكرة الايضاحية المرافقة لنصوص هذا القانون وتعديلاته المستقبلة مقدمة في التفسير عن غيرها.
- تكون المبادئ التي ترسيها المحاكم في أحكامها ملزمة حين تطبيق هذا القانون. وعند وجود تنازع بين مبادئ مستمدة من هذا القانون يكون لمحكمة الموضوع الفصل في هذا التنازع في الدعوة المنظورة. ويجب على محكمة الموضوع ومن تلقاء نفسها احالة التنازع المذكور الى المحكمة العليا/ الدائرة الدستورية إذا كان هذا التنازع قائما بين مبدأ او مباديء تستند الى هذا القانون ومباديء مستمدة من القوانين الاخرى. ويجوز أن يكون الدفع بوجود تنازع بين المباديء سندا للبراءة والإدانة، وفي هذه الحالة الأخيرة يسري هذا السند فيما يتعلق بالدعاوى السابقة إذا كان الحكم فيها بالإدانة.

مادة (3)
تفسير النصوص

يراعى في تفسير المصطلحات الواردة في هذا القانون تطورات صناعات وابتكارات الحوسبة والرقمية.

مادة (4)
دعوى التفسير أمام المحكمة العليا

تُرفع دعوى أصلية لتفسير نصوص هذا القانون امام المحكمة العليا/ الدائرة الدستورية وفق الاوضاع العادية في الاستعجال، ويجب ان تفصل المحكمة العليا في هذه الدعوى خلال شهر من تاريخ رفعها.

مادة (5)
تطبيق القانون

لا يعاقب على الجرائم المرتكبة باستخدام الحوسبة والرقمية سوى بمقتضى هذا القانون. ويراعى في التشريعات الخاصة المبادئ المقررة في هذا الباب.

مادة (6)
النظام التراسلي

فيما خلا ما هو منصوص عليه صراحة في هذا القانون، او في تشريعات لاحقة، تنطبق نصوص هذا القانون فقط على الجرائم التي ترتكب باستخدام النظام التراسلي.

مادة (7)
أثر العلاقة العقدية او الترخيص

لا تنطبق أحكام هذا القانون حين قيام الغير بانتهاك علاقة عقدية ليس طرفا فيها او تجاوز اجراءات ترخيص اداري مطلوب ما لم يكن هذا الانتهاك مبنيا على أحد الأسس التالية كحد أدنى للتطبيق:

- **اختراق سنده المهارة الخاصة.**
- **توفير مناخ ارهابي او تهديد خطير للعالم الافتراضي.**
- **جريمة من جرائم الكتاب الثاني من قانون العقوبات والتشريعات ذات العلاقة المباشرة بسيادة الدولة.**
- **انتهاك الحق في الخصوصية المبني على التوقع المعقول لها.**
- **اغراق الخوادم.**
- **جرائم التزوير والتزييف المنصوص عليها في قانون العقوبات.**
- **التسبب في انتهاك اتفاقيات دولية او اقليمية او ثنائية تكون الدولة طرفا فيها او لها مصلحة في وجودها.**
- **اعاقة تحقيق دولي مفتوح له علاقة من أية نوع بالجريمة المرتكبة ولو لم يتم اكتشاف تلك العلاقة او الجريمة ككل بعد.**

مادة (8)
دور المنظمات الأهلية في مكافحة الجريمة الافتراضية

ما لم يعترض المجني عليه او المتضرر من الجريمة او وكيله على ذلك، للمنظمات الأهلية ذات العلاقة بهذا القانون ولو أكاديميا او علميا او كانت منظمات أهلية دولية او اقليمية معترفا بها في ليبيا:

1- تحريك اجراءات الدعوى المدنية التابعة ورفعها ومتابعتها.

2- الحلول محل المجني عليه في تقديم الشكوى في الدعوى الجنائية دون حاجة لوجود توكيل او تفويض منه.

3- رفع الجنحة المباشرة دون توكيل او تفويض من المجني عليه. ويشترط في هذه الحالة الأخيرة وجود مصلحة قائمة ومشروعة وفق النظام الاجتماعي والاقتصادي الليبي، ولو كانت الجريمة مرتكبة في إطار خوادم ومضيفات خارجية ما دام البث يصل الى البلاد.

الفصل الثاني
علم الاجرام الافتراضي

مادة (9)
المجرم التقني

ليس في هذا القانون ما يشير الى ان الهكترة حركة اجرامية، وان الهاكر مجرم، ما لم يكن قد ارتكب أحد الافعال المجرمة بمقتضى هذا القانون.

مادة (10)
أثر النشاط التقني

لا يعد النشاط التقني جزءا من النشاط المادي في الجرائم المقررة في هذا القانون إلا إذا ثبت في مرتكب الجريمة توافر الشروط التالية:
- أنه يملك مهارات خاصة في مجال الحوسبة والرقمية.
- أنه استخدم تلك المهارات بنفسه او بالاشتراك مع غيره في ارتكاب الجريمة عينها محل الضبط.
- أنه تجاوز عمدا بنفسه او مع غيره الصلاحيات التقنية المقررة له بحكم طبيعة عمله او بسبب وظيفته ولو كانت تلك الصلاحيات غير مدرجة في وظيفة مسماه في الملاك الوظيفي. ولا تسري هذه الفقرة الا في حالة أن يكون مرتكب الجريمة موظفا عاما او موظفا فعليا او مستخدما مؤقتا او دائما، بمقابل او بدون بمقابل، في ذات الجهة التي ارتكبت فيها الجريمة.

ولا تطبق هذه المادة حال ارتكاب الجريمة مصادفة ولو كانت نية مرتكب الجريمة ارتكاب ذات الجريمة.

مادة (11)
النشاط التقني في جرائم أمن الدولة وجرائم الاموال العامة

ما لم يوجد نص يقرر غير ذلك، لا يعد النشاط التقني جزءا من النشاط المادي في جرائم أمن الدولة وجرائم الاموال العامة وجرائم التزييف والتزوير إذا كان استخدام الحوسبة والرقمية بقصد تسهيل ارتكاب هذه الجرائم. وتنطبق احكام الكتاب الثاني من قانون العقوبات لسنة 1953 مباشرة. وتسري في شأن مرتكب النشاط التقني احكام الفاعل الاصلي للجريمة المقررة في قانون العقوبات المشار اليه إذا كان على دراية وادراك بالجريمة او إذا كان قد ارتكب هذه الجريمة بالاشتراك مع غيره ولو كان دوره في الجريمة مجرد القيام بدور تقني.

الفصل الثالث
سلطة القاضي في تقدير العقوبة

مادة (12)
العلم بالحوسبة والرقمية

في كل الأحوال يراعي القاضي في تطبيق نصوص هذا القانون معرفة ودراية المحكمة بالحوسبة والرقمية. ويلتزم قاضي الموضوع بتبرير العقوبة على أساس الفصل الأول من الباب الثاني من هذا القانون.

مادة (13)
تقدير العقوبة

يلتزم القاضي حين تقدير العقوبة بمراعاة حجم الضرر او الخطر المحدق والمستحيل دفعه خلال مدة زمنية معقولة والمترتب كأثر للنشاط الاجرامي وفق هذا القانون. وله في ذلك زيادة معدل العقوبة المالية- دون غيرها- المقدرة في النص للجريمة.

الباب الثاني
القاعدة الموضوعية

الفصل الأول
المصالح الاجتماعية الاقتصادية

مادة (14)
المصلحة أساس الحكم

يراعي قاضي الموضوع في كل الاحوال حجم المصلحة القائمة والمشروعة المعتدى عليها في كل جريمة وفي تقدير العقوبة وفق هذا القانون.

مادة (15)
البيئة التنافسية للحوسبة والرقمية

ليس في هذا القانون، او في غيره من التشريعات اللاحقة، ما يقيد البيئة التنافسية الكاملة للعالم الافتراضي. ويلزم تفسير التشريعات النافذة في الدولة بما يتواءم مع هذه المادة.

الفصل الثاني
أنواع الجرائم

أولا: الجرائم التقنية

مادة (16)
الاختراق

كل من اخترق او انتهك حاسوب مشمول بالحماية بمقتضى هذا القانون او بأي قانون آخر، سواء باستخدام مهاراته التقنية او باستخدام أساليب مادية واحتيالية لتحقيق أغراض الانتهاك الرقمي يعاقب بعقوبة منع استخدام التقنية لمدة سنة او بعقوبة اجتماعية لمدة معينة يقررها القاضي من بين:

- القيام بحملة نظافة في الشوارع والقطاعات في اطار المكان الذي بدأ منه النشاط المادي.
- القيام بتنظيف الغابات والمراعي والمدارس والميادين وغير ذلك.
- العمل بدون مقابل في أي ادارة تتقدم بطلب التحفظ على مرتكب الجريمة، وفي هذه الحالة لا تسري القواعد المنصوص عليها في قانون العمل او الوظيفة العامة خلال مدة العقوبة. وتضع الجهة التي يوافق عليها كجهة تحفظ قواعد تشغيل المخترقون وفق هذا النص.

ويعد حاسوبا مشمولا بالحماية كل حاسوب متصل بغيره من الحواسيب والشبكات المختلفة باستخدام النظام التراسلي.

مادة (17)
الدخول او تجاوز الصلاحية في الدخول بقصد ارتكاب جريمة تقليدية

إذا كان الدخول- ولو كان مشروعا او كان دخولا متجاوز الصلاحية- بقصد ارتكاب جريمة او جرائم أخرى مما هو مقرر في قانون العقوبات لسنة 1953 او أي تشريع آخر فتسري عقوبتها المقررة في التشريعات المذكورة. وتطبق العقوبة الواردة في المادة (16) السابقة على من شارك بمهاراته الخاصة في ارتكاب الجريمة التقليدية إذا كان عمله محصورا في الاختراق و...:

- كان الدخول قد تم على قاعدة بيانات خاصة يكون مرتكب الدخول غير المشروع او تجاوز الصلاحية في الدخول على دراية بها بسبب عمله.
- او كان الدخول عبر شبكات محلية لا يحتاج للدخول اليها مهارات خاصة.

وفي حالة الدخول بنية القتل تجب عقوبة الاعدام العقوبات الاخرى.

مادة (18)
استخدام التشفير بقصد التغطية على الجرائم

كل من استخدم نظم تشفير أي كانت، بسيطة او مركبة، للتغطية على ارتكاب جريمة ما بما في ذلك جرائم العدوان على المصنفات والملكية الفكرية يعاقب بالحبس وبالغرامة ويلتزم قاضي الموضوع بالفصل في الدعوى المدنية التابعة. ولا يعفي الحكم بالبراءة من الحكم بالتعويض.

مادة (19)
فك التشفير

كل من استخدم الحوسبة والرقمية بقصد فك التشفير يعاقب بالحبس والغرامة وبعقوبة اجتماعية لمدة ثلاثة شهور.
ويعد من قبل التشفير وفق هذه المادة نظم المفتاح العام وتطبيقاته في التوقيع الالكتروني وكذلك تطبيقاته في الكروت الذكية وكروت الاعتماد المصرفية وغير ذلك.

مادة (20)
اغراق الخوادم

كل من استخدم نظم الحوسبة والرقمية مستهدفا بذلك تعطيل الخوادم عن الخدمة واغراقها بقصد الاخلال بالسير الطبيعي او العادي للنظام التراسلي يعاقب بعقوبة منع استخدام التقنية لمدة ستة شهور وبعقوبة اجتماعية لمدة ثلاثة شهور.
وتكون العقوبة الحبس مدة لا تقل عن ستة شهور والغرامة التي لا تزيد عن خمسين الف دينار إذا ترتب على اغراق الخوادم خسائر من أية نوع في مؤسسات رسمية او مالية ومصرفية.

مادة (21)
اعداد شفرة فيروسية

كل من قام بإعداد او تصميم او تطوير برنامج او شفرة ضارة او ذات طابع فيروسي خطر، سواء كانت مركبة في برنامج اخر او بسيطة منفردة، يعاقب بعقوبة منع استخدام التقنية لمدة سنة.
ولا يعاقب مبتكر الشفرة الضارة او البرنامج الخطر إذا كان في ابتكاره هذا ما يؤدي الى تحقيق معدل تنموي او أكاديمي في مجال تأمين البيانات او أمن المعلومات او الخوادم والمضيفات بأي شكل كان.

مادة (22)
بث الفيروسات

كل من قام ببث عشوائي لشفرة او لبرنامج نتج عنه تعديل في نظم برمجية او معلوماتية تخص الغير- ولو كان البث في حواسيب منفرده- وترتب على ذلك فقدان مصداقية هذه النظم بأي شكل من الأشكال يعاقب بعقوبة منع استخدام التقنية لمدة ثلاثة شهور والغرامة التي لا تقل عن اربعة الاف دينار ولا تجاوز العشرة الاف دينار. ولا أهمية في هذه الحالة لمدى قيام الغير بتأمين او استخدام نظم أمن المعلومات ومدى تطورها في حواسيبه ما دام البث عشوائيا.
وما لم يثبت ان السبب هو الترويج التجاري لمضادات الفيروسات وبرامج تأمين البيانات وأمن المعلومات فإنه يعفى الفاعل من العقاب إذا ثبت أنه قام بتوجيه الشفرة الخطرة او الضارة الى شبكة

معينة او حاسوب معين دون غيره ولم تكن تلك الحواسيب مؤمنة وفق النظم الحديثة في تأمين البيانات او امن المعلومات.

مادة (23)
البريد الدعائي المحظور

كل من استخدم نظم البريد الدعائي المحظور دون تصريح وبغير الالتزام بالقواعد التقنية المقررة لذلك وترتب على ذلك احتكار ولو مؤقت لحركة النظام التراسلي يعاقب بالغرامة حدها الاقصى عشرة الاف دينار.
وإذا احتوى البريد الدعائي المحظور على مواد دعائية غير مشروعة او مخالفة للقانون والآداب العامة والحياة الاجتماعية والسياسية تكون العقوبة الحبس والغرامة.
وتكون العقوبة السجن إذا كان الاستخدام بغرض نشر أفكار ارهابية ومناهضة للمباديء العليا للهيئة الاجتماعية.

ثانيا: جرائم العدوان على التخزين الرقمي

مادة (24)
التداول غير المشروع للبيانات الاسمية

كل من قام بنشر او بث لبيانات اسمية تخص الغير او استخدمها في أعماله او تجارته بمقابل او بدون مقابل بغير موافقة صريحة ومكتوبة من صاحبها يعاقب بالغرامة حدها الاقصى عشرة الآف دينار.

كل من استولى على بيانات اسمية بطرق رقمية او مادية واستخدمها في ارتكاب جريمة من الجرائم المنصوص عليها في الفقرة الاولى السابقة يعاقب بالحبس مدة شهر وغرامة عشرة الآف دينار.
وتكون العقوبة الحبس مدة لا تقل عن سنتين والغرامة إذا كان مرتكب الجريمة موظفا عموميا او مستخدما لدى احدى الجهات الرسمية.
ويعد من قبل البيانات الاسمية الصور والوثائق التي تخص الغير ما لم تكن متخذة طبيعة الوثائق العامة او جزءا منها.
وتعد الموافقة الرقمية والشفوية الصريحة او الضمنية من قبل صاحب البيانات في مرتبة الموافقة الكتابية.

مادة (25)
الدخول غير المصرح به على قواعد البيانات الاسمية

يعاقب بالسجن والغرامة كل من استخدم مهاراته في الحوسبة والرقمية دون تصريح او مشروعية مستهدفا الدخول والاطلاع على قواعد بيانات اسمية يقرر القانون حصانتها وخصوصيتها مثل:

- الأحوال المدنية.

- التسجيل العقاري.
- قواعد بيانات المستشفيات وبنوك الدم والهيئات الصحية والعلمية والبيولوجية.
- المؤسسات العامة والعسكرية.
- المؤسسات الأمنية والسياسية.
- مصرف ليبيا المركزي.
- المؤسسات الاخرى التي يقرر لها القانون هذه الحصانة.

وتكون العقوبة السجن المؤبد إذا كان مرتكب الجريمة موظفا او مستخدما في تلك المؤسسات وتجاوز صلاحياته في الدخول على البيانات المذكورة.
وتكون العقوبة الاعدام إذا كان ارتكاب الجريمة بغرض التجسس لمصلحة دولة أجنبية او نجم عن الدخول وفق هذه المادة وفاة او قتل جماعي او تخريب مؤدي الى ذلك او ايذاء خطير او كارثة.

مادة (26)
الاطلاع على البيانات السرية

كل من إطلع على بيانات رقمية معدة سرية وفق النظم الأمنية المعمول بها في ليبيا، دون أن يكون له الحق في ذلك، يعاقب بالحبس مدة لا تزيد عن شهر وبعقوبة منع استخدام التقنية المدة التي يقررها قاضي الموضوع. ويجوز اتخاذ الاجراءات وفق ما هو مقرر في المادة (187 مكرر) وما بعدها من قانون الاجراءات الجنائية.
ولا تقوم الجريمة أصالة إذا تداخلت الصدفة او ثبت ان بث تلك البيانات رقميا سببه جريمة سابقة على وقوع فعل الاطلاع.
ولا يشترط في هذه المادة ان تكون البيانات الرقمية مرتبطة بالنظام التراسلي.

مادة (27)
ازالة واتلاف الأدلة الرقمية

تطبق الاحكام المتعلقة باتلاف الدليل الواردة في قانون العقوبات والتشريعات الاخرى على جرائم ازالة واتلاف الدليل الرقمي. ومع ذلك تسأل الجهة الملزمة بالتحفظ واستخلاص الدليل الرقمي إذا لم تتخذ الاجراءات التقنية الكفيلة بالمحافظة على الدليل المدة اللازمة لذلك إذا ترتب على ذلك ضياع حقوق للغير بما في ذلك المؤسسات والجهات العامة والمجتمع. ويكون على هذه الجهة اثبات انها اتخذت هذه الاجراءات المشار اليها للحفاظ على الدليل.
ومع مراعاة المادة (79) من هذا القانون تحدد مدد التحفظ واستخلاص الدليل الرقمي بقرار من اللجنة الشعبية العامة للعدل بناء على توصية اللجنة المحددة في قانون الاصدار.

مادة (28)
اتلاف الجاني للأدلة الرقمية

كل من قام باتلاف دليل رقمي يمكن ان يحقق ادانة او براءة للنفس او للغير في اجراءات جنائية صحيحة يعاقب بالحبس مدة لا تقل عن ستة شهور وبغرامة عشرين ألف دينار.

ويعاقب بالحبس مدة لا تقل عن سنة والغرامة عشرة آلاف دينار كل من أتلف دليلا رقميا في دعوى غير جنائية.
وتكون العقوبة مساوية لعقوبة الجاني إذا كان الدليل الرقمي هو الدليل الوحيد في الدعوى الجنائية وغيرها. ولا تسري هذه الفقرة إذا كان مرتكب جريمة الاتلاف من أقارب الجاني حتى الدرجة الثانية.

مادة (29)
حيازة قطع صلبة او مرنة محظورة

كل من حاز او أحرز قطع صلبة او مرنة محظورة كانت او غير مشروعة ولا يجوز حيازتها او احرازها رقميا او ماديا إلا بتصريح خاص من جهة عامة يعاقب بغرامة لا تتجاوز مائة ألف دينار. ويتم التحفظ على القطع الصلبة او المرنة الى حين استخراج التصاريح او التراخيص اللازمة.
وتلتزم الجهة التي قامت بالتحفظ على هذه القطع بحفظها بما يتوافق وطبيعتها خلال المدة المقررة لاستخراج التصاريح او التراخيص، وفي حالة الاخلال بهذه الفقرة تلتزم الجهة المذكورة بالتعويض.

ثالثا: جرائم المخدرات والغسل الرقمي للأموال

مادة (30)
الترويج للمخدرات والمؤثرات العقلية باسلوب تقنية المعلومات

كل من قام بالترويج غير المشروع للمخدرات والمؤثرات العقلية باستخدام الحوسبة والرقمية يعاقب بالسجن مدة لا تقل عن خمسة عشر عاما والغرامة التي لا تقل عن خمسين ألف دينار.
ويعاقب بالسجن المؤبد وبغرامة لا تقل عن مائة ألف دينار معد برمجية الترويج ومعد الصفحات بنظام شبكة المعلومات الدولية وكذلك الوسيط الالكتروني الذي نشرت الصفحات من خلال موقعه على الانترنت او الملقم التابع له وتضمنت كليا او جزئيا ترويجا غير مشروع من أي نوع للمخدرات والمؤثرات العقلية.
ويقصد بالترويج في نطاق هذه المادة هو كل تعريف بالمخدرات والمؤثرات العقلية بين الناس بقصد اغوائهم واغرائهم وتحريضهم على التعاطي والادمان او الاعتماد خاصة والتعامل بالمخدرات والمؤثرات العقلية على
العموم وذلك بتعريفهم بكيفية زراعتها او تنميتها او تطويرها او تخليقها معمليا او اعدادها للتعاطي وكيفية تعاطيها والمدة اللازمة بين الجرعة والاخرى.

مادة (31)
الاتجار بالمخدرات والمؤثرات العقلية بنظام البريد الالكتروني

كل من قام بالاتجار غير المشروع بالمخدرات والمؤثرات العقلية وكانت وسيلته للتعرف على الطلب او طريقته في التسليم هى مراسلات البريد الالكتروني يعاقب بالإعدام.

مادة (32)
استخدام نظم التجارة الالكترونية في الاتجار غير المشروع

كل من استخدم نظم التجارة الالكترونية بقصد الاتجار غير المشروع بالمخدرات والمؤثرات العقلية يعاقب بالإعدام.
ويعاقب بالسجن المؤبد، وغرامة تعادل ضعف قيمة المعاملة، كل من استخدم نظم الحوسبة والرقمية بقصد الاتصال بمنظمات الاتجار غير المشروع بالمخدرات والمؤثرات العقلية وكان غرضه التعامل في المخدرات والمؤثرات العقلية مع افراد هذه المنظمات.
وتطبق المواد (4- 5- 6) من قانون العقوبات لسنة 1953 والمادة الاولى مكرر من قانون المخدرات والمؤثرات العقلية على المتعامل بنظام التجارة الالكترونية لهذا الغرض من خارج الآراض الليبية إذا ثبت قيامه بمعاملات توريد مع مؤسسات في داخل البلاد بقصد التعامل بالمخدرات والمؤثرات العقلية.
وإذا كان الضحية ناقص الاهلية فلا تسقط الاجراءات الجنائية بالتقادم.

مادة (33)
عقوبات تبعية

يحرم من الحقوق الرقمية كل من حكم عليه بمقتضى المواد السابقة. وفي كل الاحوال يجوز الحكم بالمصادرة الدائمة لكافة وسائل الحوسبة والرقمية المستخدمة في التعامل غير المشروع بالمخدرات والمؤثرات العقلية بمقتضى التشريعات النافذة في الخصوص.
ويجوز بمقتضى قرار مسبب من رئيس النيابة العامة القيام باتخاذ اجراء تحفظي أو أكثر على تلك المعدات بواسطة خبراء في تقنية المعلومات والحاسوب، مع ضرورة اتخاذ اجراءات تقنية هدفها التحفظ على البرمجية او الموقع او الصفحة القائمة على الانترنت الى حين صدور حكم قضائي بإزالتها.

مادة (34)
عقوبة تبعية على استضافة مواقع مخدرات ومؤثرات عقلية وأدوية

يعد وسيطا الكترونيا- وفق هذا الفصل- كل شخص طبيعي او اعتباري يملك الوسائل اللازمة للتعامل كحلقة وصل او شبكة بقصد تقديم خدمات الانترنت.
ويحكم دائما بالغلق وحرمان الوسيط الالكتروني مستقبلا من الترخيص كمزود إذا لم يثبت الوسيط المذكور أنه اتخذ الاجراءات التقنية اللازمة لمنع استضافة مثل تلك المواقع. وفي كل الاحوال يحكم بالنشر وتعميم الحكم الصادر بالإدانة او البراءة.
وإذا كان موقع الوسيط الالكتروني خارج البلاد تتخذ الاجراءات الجنائية ضده بما هو مقرر في التشريعات النافذة والاتفاقيات الدولية التي تكون ليبيا طرفا فيها.
ولا تسقط الاجراءات الجنائية المتخذة ضد الوسيط الالكتروني بالتقادم إذا اتخذت أية اجراءات ولو ادارية في أثناء المدة المقررة قانونا لذلك.

مادة (35)
البلاغ

لا تتخذ الاجراءات الجنائية ضد المبلغ عن الجرائم المقررة في المواد من (30) وحتى (34) من هذا القانون ولو كان المبلغ هو المتعاطي او المعتمد على المخدرات والمؤثرات العقلية او كان البلاغ رقميا او كان مقدما الى جهة أهلية او مصحة لعلاج المدمنين، مع احتفاظ المبلغ بالحق في السرية وعدم الاعلان عن شخصيته.
وتعد أقوال المتعاطي او المعتمد أثناء العلاج من قبيل المعلومات السرية التي لا يجوز الاستناد اليها في الادانة.

مادة (36)
المراهنات والتحايل بهدف غسل الأموال

كل من قام باعداد مواقع قمار او مراهنات عبر الانترنت او مزادات مختلفة باستخدام شبكة المعلومات الدولية او أية شبكات خاصة اخرى او مواقع لوتريا او أنشأ مؤسسات مالية افتراضية ذات طابع احتيالي او غيرها يعاقب بالسجن والغرامة التي لا تقل عن مائة الف دينار وغلق الخادم وحجب الموقع. ويعاقب بذات العقوبة كل من تحايل على مؤسسات مالية بفتح حسابات الكترونية او رقمية فيها مستهدفا بذلك القيام بعمليات غسل الاموال
او جذب عملاء غسل الأموال. ويلزم الحكم بمصادرة الاموال محل الغسل والحكم بغلق المؤسسة او الموقع او الخادم.
ويتم تعميم الحكم الصادر بمقتضى هذه المادة على الجهات المحلية والدولية ذات العلاقة.

مادة (37)
معاقبة الشريك في غسل الأموال

كل من قدم استشارات فنية او تقنية لمرتكب جريمة غسل الأموال الرقمي او قام بمساعدة مرتكبيها وقدم لهم التسهيلات المادية والدعم الفني والتقني بأي شكل من الاشكال يعد شريكا في الجريمة إذا ارتكبت الجريمة فعلا وكان دور الاستشاري واضحا فيها. وتطبق احكام الاشتراك الواردة في قانون العقوبات لسنة 1953. وإذا كان الاستشاري مؤسسة او مكتب يحكم بالغلق.
ويعد شريكا في الجريمة من يتواجد لديه ملفات مخزنة لعمليات غسل الأموال ولم يبلغ عنها الجهات المختصة. ولا تسري هذه الفقرة على المرؤوس الذي ينفذ تعليمات التخزين ولو كان ذلك بأساليب التشفير ما لم يكن على دراية بمحتوى تلك الملفات.

رابعا: جرائم العدوان على الاخلاق

مادة (38)
اعداد وتصميم مواقع اباحية

كل من قام بتصميم صفحات النشر الفاضح وإعداد مواقع اباحية عبر الانترنت او استخدم وسائط التخزين المختلفة او استخدم التهجين الرقمي في تنفيذ نشاطه او شارك في تنفيذ ذلك بأي شكل من الاشكال وكان ذلك بقصد الاتجار فيها يعاقب بمنع استخدام التقنية مدة اربع سنوات وبالحبس مدة لا تزيد عن ثلاثة شهور. وتكون العقوبة الحبس إذا تبين ان محل التصميم او التخزين او غير ذلك أشخاص طبيعيون.

مادة (39)
استضافة مواقع مغرضة

يعاقب بالسجن مدة لا تقل عن خمسة سنوات ومصادرة الخوادم والمضيفات المعدة لذلك كل من قام في القطر الليبي بإعداد مضيفات او خوادم خاصة لاستضافة وتخزين وبث:

- مواد اباحية لأشخاص طبيعيين، بمقابل او بدون مقابل.
- مواد تحرض على العنصرية او التفرقة او الكراهية.
- مواد احتيالية او نصب او بث برامج وادوات تساعد على ذلك.
- مواد تحتوي عدوانا على الملكية الفكرية او تساعد على ذلك.
- مواد تقلل من شأن دين من الاديان السماوية او تتضمن اساءة او نقد للانبياء او الرسل او تعرض للشخصيات التاريخية الكبرى بشكل غير صحيح وبغير ما هو مقرر لهذه الشخصيات من حرمة.
- مواد سرية كانت او غير صحيحة تتعرض للنظام السياسي والاجتماعي والاقتصادي للهيئة الاجتماعية ومؤسساتها بشكل يفقد الدولة مصداقيتها في المجتمع المحلي والدولي.
- مواد ارهابية.

مادة (40)
التحريض على الاباحية

كل من قام باستخدام البدائل المختلفة للحوسبة والرقمية من تراسل وتخزين بقصد التحريض على ارتكاب أفعال اباحية وجنسية مع الغير او قام باستدراجه للقيام بذلك بأن يطرح الجاني للغير صور اباحية ثابتة كانت او متحركة بالصوت والصورة او يعرض نفسه فيها او عبر الوسائط المتعددة او يستعرض قدراته الجنسية او يغوي الغير او يحرض على ايجاد تجمعات اباحية سرية او علنية او يحرض على الاباحية بصورة عامة يعاقب بالسجن مدة لا تزيد عن خمس سنوات.
وتكون العقوبة السجن مدة لا تقل عن سبع سنوات إذا كان من بين المجني عليهم قاصرا او من ذوي الاحتياجات الخاصة او كان فيه عيب في الادراك او ممن يخضع لنظم علاجية خاصة او ممن يخضع لوصاية نتيجة لإصابته بمرض عقلي.

وتكون العقوبة السجن مدة لا تزيد عن خمسة عشر سنة إذا قام الجاني بمطاردة او ازعاج المجني عليه سواء رقميا او ماديا.

مادة (41)
اساءة استخدام البريد الالكتروني والاتصال المباشر

تطبق أحكام السب والقذف المقررة في قانون العقوبات على كل من يستخدم حساب البريد الالكتروني وبرامج الاتصال المباشر في توجيه سب او قذف مباشر الى الغير او اتهامات غير صحيحة او كان في تلك المراسلات الالكترونية او الأحاديث المباشرة اساءة من أية نوع.
ولا تسري هذه المادة في حالة المنازعات العائلية والاجتماعية العادية او كانت الالفاظ المستخدمة دارجة في إطار الخطأ الاخلاقي الشائع او كانت العادة بين الجاني والمجني عليه سند ذلك، او الحالة التي يثبت فيها ان توجيه السب او القذف او التشهير او التهديد او الاساءة ناجم عن مجهول سطا على الحساب الشخصي.
ولا يجوز رفع الدعوى الا بناء على شكوى الطرف المتضرر وفقا للمادتين (3- 18) من قانون الاجراءات الجنائية.
ويراعى في تحريك الدعوى الجنائية وفقا لهذه المادة ما هو مقرر في المادة (90) من هذا القانون.

مادة (42)
التشهير

في غير حالات استخدام المواقع الاعلامية والصحفية الالكترونية او الرقمية تطبق أحكام التشهير الواردة في قانون العقوبات لسنة 1953 على كل من قام- بغرض التشهير بالغير- ببث ونشر موضوعات وصور ووسائط متعددة في مواقع او استخدم حساب بريد الكتروني صوري او نظم الاتصال المباشر.

مادة (43)
التشهير عن طريق بوابات اعلامية وصحفية

إذا كان التشهير قد تم عبر بوابات اعلامية او صحافة الكترونية او رقمية يعاقب مرتكب الجريمة بعقوبة الحبس.
ويشترط في هذه الحالة أن يكون التشهير موجها الى الذات وان يتقدم المتضرر من الجريمة بشكوى وفقا للمادتين (3- 18) من قانون الاجراءات الجنائية.
ويعاقب بذات العقوبة المدير المسئول عن النشر في البوابة او الموقع إذا ثبت ان المتضرر من الجريمة قد طالبه بإزالة التشهير ولم يقم بذلك خلال اسبوع من المطالبة ما لم يثبت ان التشهير قد طال صفة المجني عليه وليس ذاته. ولا يجوز تحريك الدعوى الا بشكوى الطرف المتضرر.
وإذا كان التشهير مساسا بالأشخاص المذكورين في المادة (195) من قانون العقوبات تطبق العقوبة الواردة في تلك المادة دون تمييز بين ذات المجني عليه وصفته.
ولا تخضع للتقادم جريمة التشهير وفق هذه المادة.
ويجب في كل الاحوال الفصل في الدعوى المدنية التابعة في ذات الحكم الصادر بالإدانة أو البراءة.

مادة (44)
التهديد عبر الانترنت

كل من قام بتهديد الغير بأية صيغة كانت وذلك باستخدام البدائل المختلفة للحوسبة والرقمية يعاقب بالحبس والغرامة.
وتكون العقوبة السجن إذا تحقق التهديد في صورة نشاط مادي او رقمي. ويعد شريكا ويعاقب بذات العقوبة مرتكب الواقعة المادية والرقمية إذا لم يكن هو المصدر الرئيسي للتهديد وانحصر دوره في التنفيذ.
وتكون العقوبة السجن المؤبد إذا ترتب على التهديد كارثة محققة او اضرار او أخطار أي كانت.
ولا تقام الدعوى الا بشكوى الطرف المتضرر.

خامسا: جرائم العدوان على الحق في الخصوصية

مادة (45)
العدوان على الحق في الخصوصية

كل من استخدم مضيفات او خوادم محلية لاختراق حواسيب مشتركة فيها يعاقب بمنع استخدام التقنية لمدة ثلاثة سنوات. ويضاف الى هذه العقوبة عقوبة الحبس إذا كان مرتكب الجريمة من العاملين في اطار ادارة الخادم او المضيف المحلي الذي تم من خلاله الاختراق، ولم يكن لديه مبرر لذلك.
ولا تنطبق هذه المادة إذا كانت الشبكة المحلية داخلية وكان ذلك بقصد مراقبة اعمال الوظيفة في مؤسسة او جهة معترف بها قانونا او كانت الجريمة محلها منازعات العائلية.

مادة (46)
مراقبة حركة الاتصال المباشر

كل من قام باتخاذ اجراءات تقنية مادية او رقمية بغرض مراقبة حركة الاتصال المباشر بين الافراد والمؤسسات دون مبرر مشروع، بمقابل او بدون مقابل، يعاقب بعقوبة منع استخدام التقنية لمدة ثلاث شهور وعقوبة اجتماعية يقررها قاضي الموضوع ويحكم بالغلق إذا كانت المراقبة تتم من خلال مؤسسة او مكتب اتصالات قائم بغير تصريح.
ويعد من قبل مراقبة حركة الاتصال المباشر القيام ولأغراض تجارية باستخدام تقنيات الانترنت لفتح خطوط الهاتف الرقمي دوليا دون تصريح.
ولا تقوم الجريمة إذا كان استخدام الهاتف الرقمي دوليا من المنازل ودون غرض تجاري.

مادة (47)
السطو على البريد الالكتروني

كل من سطا على حساب بريد الكتروني بقصد التعرف على مضمون ومحتوى مراسلات الكترونية خاصة بالغير دون ان يكون له الحق في ذلك يعاقب بالحبس وبغرامة لا تجاوز عشرة آلاف دينار ويلزم لتحريك الاجراءات الجنائية شكوى الطرف المتضرر. ويعفى الفاعل من العقاب إذا ثبت توافر الشروط التالية:

- **ان ما قام به هو مجرد اثبات مهارة مثل كسر كلمة العبور حساب البريد الالكتروني.**
- **انه لم يستخدم حساب البريد الالكتروني في ارسال رسائل الكترونية من اية نوع ولو كانت حسنة النية.**
- **أنه لم يقم بالاطلاع على مراسلات الكترونية ثبت قيام صاحب الحساب بفتحها من قبل.**
- **كذلك يعفى الفاعل من العقاب إذا ثبت وفاة حائز حساب البريد الالكتروني، إذا كان من أقاربه حتى الدرجة الثانية، وكان هناك دليل على مصلحة عائلية في حساب البريد الالكتروني للمتوفي..**

وإذا ثبت قيام مرتكب الفعل بالاطلاع على مراسلات الكترونية لم يقم صاحب الحساب بفتحها والاطلاع على محتواها حتى زمن ارتكاب الجريمة فإنه يلزم لتحريك الدعوى الجنائية ضد مرتكب الفعل وفقا لهذه المادة شكوى مزود الخدمة او الوسيط. ويسأل الوسيط في هذه الحالة مسئولية رقمية عن تأمين البيانات ونظم أمن المعلومات ومدى جدارتها للقيام بدروها.

سادسا: جرائم الاحتيال

مادة (48)
الاحتيال

كل من استخدم طرق احتيالية عبر البدائل المختلفة للإنترنت للحصول على كسب غير مشروع أيا كان، ماديا او معنويا او رقميا، يعاقب بعقوبة منع استخدام التقنية مدة لا تقل عن ثلاثة سنوات ولا تزيد عن عشرة والغرامة خمسون ألف دينار.
وإذا كان مرتكب الجريمة يتبع شخص اعتباري او افتراضي تكون العقوبة الحبس لمدة ستة شهور وازالة الموقع او الغلق حسب الاحوال.
ويلزم نشر الحكم الصادر بالإدانة على نفقة مرتكب الجريمة في وسائل الاعلام المختلفة بما في ذلك الموقع الاحتيالي ذاته.

مادة (49)
الاحتيال بالمبالغ الصغيرة

كل استخدام للعالم الافتراضي لطرح لوتريا او يانصيب او نظام جوائز أي كان بهدف جني الأموال باستخدام نظام المبالغ الصغيرة دون تصريح بذلك من الجهات المختصة يعاقب بالحبس وبعقوبة اجتماعية لمدة ثلاثة شهور.

مادة (50)
نشر الحكم

يلزم نشر الحكم الصادر بالإدانة وفق المادتين (48) و (49) السالفتين على نفقة مرتكب الجريمة في وسائل الاعلام المختلفة بما في ذلك الموقع الاحتيالي ذاته.
ويجوز لمنظمات المجتمع المدني ذات العلاقة بتطبيق هذا القانون رفع ومتابعة الدعوى المدنية التابعة باسمها واستلام التعويض والتصرف فيه.

مادة (51)
الاحتيال عدوانا على نطاق الاسماء

كل من قام بتسجيل نطاق اسم Domain Name بسوء نية او بقصد الحصول على كسب غير مشروع أيا كان وبأي قيمة كانت وسواء كانت مادية او معنوية، يعاقب بالحبس والغرامة قدرها عشرين ألف دينار. ولا تقام الدعوى الا بناء على شكوى الطرف المتضرر. ويجوز ايقاف الاجراءات إذا وجد في اوراق الدعوى دلالة على تسوية بين الجاني والغير او رفع دعوى تحكيم رقمي.

سابعا: جرائم التلاعب الرقمي/ التزوير والتزييف الالكتروني

مادة (52)
التلاعب بالمستندات الرسمية

كل من تلاعب رقميا ببيانات رسمية حكومية او أمنية او اقتصادية او سياسية ليست من طبيعة عامة ويلزم للاطلاع عليها صفة خاصة، ولو كانت مخزنة في حاسوب منفرد، يعاقب بالسجن المؤبد إذا ترتب على هذا التلاعب تعريض مصالح البلاد للخطر او الاضرار بالمركز السياسي او الاقتصادي او القانوني للدولة. ولا تسقط هذه الجريمة بالتقادم.

مادة (53)
التلاعب بالمستندات ذات القيمة الاقتصادية

كل من تلاعب رقميا ببيانات- ولو كانت مخزنة في حاسوب منفرد- مستهدفا بذلك تشويه مستندات ذات قيمة اقتصادية دون أن يكون له الحق في ذلك وبقصد تحقيق كسب غير مشروع له او خسارة مالية او اقتصادية للغير تتجاوز آلف دينار يعاقب بالعقوبات المقررة للتزوير في قانون العقوبات الصادر سنة 1953.
ويعد من قبيل البيانات ذات القيمة الاقتصادية كافة المستندات ذات الطبيعة الحكومية او العامة وكذلك المستندات التي تتضمن المعاملات المالية والمصرفية التي تتم من خلال المؤسسات ويترتب على التلاعب بها فقدان ملكية او ضياع حقوق مادية او معنوية للغير. ويشمل التلاعب عدم أحقية الشخص في تعديل محتوى المستند او البيانات. ويكون من بين وسائل اثبات التلاعب رقميا او الكترونيا إذا ثبت قيام الشخص باستخدام برامج او ادوات رقمية خاصة تشتمل على أوامر ذات

علاقة بتعديل محتوى المستند الالكتروني او الرقمي بحيث يترتب على تحميلها على نظام الحاسوب حدوث التعديل ولو في اوقات مختلفة عن زمن التحميل.

مادة (54)
التلاعب بحركة العملة الرقمية

كل من تلاعب رقميا ببيانات مهيأة كعملة رقمية او لحركة تداولها على أية شاكلة تكون عليها هذه الحركة، سواء الكترونية او رقمية او ذكية، بقصد الاستيلاء عليها يعاقب بالسجن مدة لا تقل عن عشرة سنوات والغرامة تعادل ضعف المبالغ المتضررة من التلاعب.
ويعاقب بذات العقوبة كل من ثبت استخدامه لبرامج او برمجيات او أدوات خاصة بقصد ارتكاب او تسهيل ارتكاب عمليات تزييف العملة المادية. ويعد شريكا في هذه الفقرة من قام بإعداد وتصميم البرنامج او الاداة او أي جزئية فيها تساعد في ارتكاب الجريمة إذا ارتكبت فعلا. وتشمل العملة المادية وفق هذه الفقرة كروت الاعتماد وغيرها مما يمكن أن يحل محل العملة في التعامل ما دام يمكن ترجمته بشكل فوري الى نقود متداولة حول العالم.

ثامنا: جرائم العدوان على الملكية الفكرية

مادة (55)
العدوان على المصنفات

كل من قام بنشر رقمي لبرامج تخزين او تراسل او لمصنفات غير مملوكة له او دون وجه حق او بثها بمقابل او بدون مقابل في وسائط تخزين او عبر المواقع ولو لم يكن اي منها موقعه الخاص او كانت مواقع خاصة يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن عشرين ألف دينار.
وتزاد العقوبة بمقدار الثلث إذا كان مرتكب الجريمة هو الذي قام بأعمال التخزين.

مادة (56)
العدوان على قواعد البيانات

كل من قام ببث رقمي لقواعد بيانات مشمولة بالحماية ودون أن يكون له حق في ذلك او بشكل غير مشروع يعاقب بالحبس مدة لا تقل عن سنتين. وتكون العقوبة الحبس إذا قام مرتكب الجريمة بالاتجار فيها، بمقابل او بدون مقابل، في أقراص او وسائط تخزين أيا كانت.
وفي كل الاحوال تزاد العقوبة الى الثلث إذا كان مرتكب الجريمة هو من قام بإجراء التخزين او النسخ الضوئي لها وقام باستخدام برامج وأدوات الترتيب بقصد التحايل اعتمادا على محتوى قواعد البيانات.

مادة (57)
تسهيل وجود برامج وأدوات رقمية

كل من قام ببث رقمي لبرامج او أدوات رقمية تسهل انتهاك حقوق الملكية الفكرية يعاقب بالحبس والغرامة التي لا تقل عن عشرين ألف دينار.
وتزاد العقوبة الى الثلث إذا كان مرتكب الجريمة هو مبتكر هذه البرامج او الأدوات الرقمية.

الفصل الثالث
المسئولية الجنائية

مادة (58)
المسئولية الرقمية

المسئولية الرقمية مبرر للدعوى المدنية التابعة.

مادة (59)
الاهلية الرقمية

لا يعتد في تطبيق أحكام هذا القانون بقواعد الاهلية المقررة في قانون العقوبات ما لم تكن الجريمة الافتراضية تستهدف جريمة تقليدية.

مادة (60)
الباعث

مع مراعاة المادة (95) من قانون العقوبات يعتد بالباعث إذا كان لذلك سبب تقني، ويعد من قبيل السبب التقني التحدي بين الهكرة والابتكار إذا تجاوز الحدود المعقولة للإباحة.

مادة (61)
أشخاص القانون

تسري نصوص هذا القانون على الشخص الطبيعي والشخص الاعتباري. وليس في هذا القانون ما يبرر عدم الاعتراف بالشخص الرقمي.

مادة (62)
الاشتراك والتنظيمات العصابية

مع مراعاة أحكام الاشتراك المقررة في قانون العقوبات يعد مسئولا عن الجريمة وفق هذا القانون من ارتكبها بنفسه او مع غيره.

ولا يعد تنظيما عصابيا رقميا وفق هذا القانون سوى التنظيم الذي تتحدد اغراضه في كونه يتمتع بصفة الاستمرار مع تحديد الاهداف التي قام من أجلها او كانت له جذور في الواقع المادي كعصابة منظمة او من اتباع الجريمة المنظمة.

مادة (63)
مسئولية الطرف الثالث

لا يسأل الطرف الثالث عن كافة الانشطة التي يقوم بها الغير ما لم ينص صراحة على غير ذلك. ومع ذلك يجوز مسألة الطرف الثالث كشريك سلبي إذا لم يتخذ الحيطة والحذر التقني في مجال الجرائم الاخلاقية وجرائم الملكية الفكرية والجرائم المرتكبة ضد شخصية الدولة وأمنها وفق التشريعات النافذة. وتكون مسئوليته كفاعل او شريك إذا كان على دراية وإدراك بالجريمة وتعد مساهماته التقنية مساهمة فاعل في الجريمة. وفي الحالات الاستثنائية المذكورة يكون الحكم بإغلاق الطرف الثالث وجوبيا.

الفصل الرابع
العقوبات الرقمية

مادة (64)
العقوبات التقليدية

ليس في هذا القانون ما يمنع تطبيق عقوبة تقليدية كلما وجد نص فيه يستدعي هذا التطبيق. والعقوبات التقليدية هي المنصوص عليها في قانون العقوبات والتشريعات الخاصة الاخرى، وعلى الترتيب المقرر لنوعية الجرائم التقليدية.

مادة (65)
انواع العقوبات في هذا القانون

العقوبات الاصلية في هذا القانون على النحو التالي:
- العقوبات الرقمية.
- العقوبات التقليدية.
- العقوبات المالية.
- العقوبات الاجتماعية.

مادة (66)
العقوبات والتدابير الرقمية

تطبق العقوبات والتدابير الرقمية أصالة في كل جريمة منصوص عليها في هذا القانون. والعقوبات والتدابير الرقمية هي:
- منع استخدام التقنية بشكل دائم او مؤقت.
- الوضع تحت المراقبة الالكترونية.

- قطع الخدمة وإغلاق الخوادم ومصادرة محتوى المضيفات.
- حجب المواقع.
- حذف بيانات او برامج.
- مصادرة القطع الصلبة والمرنة.
- أية عقوبات اخرى يتم استحداثها مستقبلا.

مادة (67)
العقوبات المالية

العقوبات المالية المقررة في هذا القانون هي تلك التي يعترف بها قانون العقوبات. وتعد بمقتضى هذا القانون عقوبات أصلية. ومن ذلك:

- الغرامة.
- المصادرة.
- الغلق.

مادة (68)
العقوبات الاجتماعية

العقوبات الاجتماعية هي تلك التي يقررها قاضي الموضوع ويرى انها مناسبة للحالة الاجتماعية والاقتصادية والعلمية لمرتكب الجريمة. وهدفه في ذلك تحقيق معدل تنموي في درجة الوعي الاجتماعي والعلمي بالمجتمع وأهمية اندماجه في بيئته الاجتماعية المحلية والوطنية مع الاخذ في الاعتبار الطبيعة العالمية للبيئة الرقمية. وتحقق العقوبة الاجتماعية أهدافها بالتالي:

- زيادة وعي مرتكب الجريمة الافتراضية بالبيئة الاجتماعية عن طريق إلزامه بأعمال تهم البيئة الصحية في الاماكن العامة في البلاد.
- العمل على رفع معدل وعي مرتكب الجريمة بأهمية البيئة الرقمية في بيئته المحلية.
- احترام النظام الاخلاقي المحلي باعتباره عنصرا جوهريا في النظام الاخلاقي العالمي.

مادة (69)
جمع العقوبة الاجتماعية بغيرها

يجوز الجمع بين العقوبات الاجتماعية وغيرها من العقوبات، وفي هذه الحالة يلزم أن يكون الحكم بالعقوبة مستندا الى بحث اجتماعي اقتصادي لحالة الشخص مرتكب الجريمة.
ويكون تنفيذ العقوبة الاجتماعية تحت اشراف قاضي التنفيذ. ويجوز لقاضي التنفيذ تعيين ولي الامر او الوصي او القيم مسئولا عن تنفيذ العقوبة الاجتماعية إذا كان مرتكب الجريمة ناقص الأهلية لأي سبب كان.
وفي حالة عدم قيام المحكوم عليه بتنفيذ العقوبة الاجتماعية يجوز لقاضي التنفيذ احالة أوراقه الى النيابة العامة لتوجيه اتهام بمخالفة المادة (277) من قانون العقوبات.

مادة (70)
مصادرة القطع الصلبة والمرنة

ليس في هذا القانون ما يجيز مصادرة القطع الصلبة والمرنة. ومع ذلك يجوز الحكم بالمصادرة في الاحوال التالية:

- **إذا كانت الجريمة المرتكبة من الجرائم الماسة بشخصية الدولة وفق أحكام البابين الأول والثاني من الكتاب الثاني لقانون العقوبات.**
- **الجرائم الاخلاقية والإباحية وجرائم العدوان على الحق في الخصوصية والبيانات الاسمية والتشفير.**
- **جريمة دولية او ذات طابع دولي.**

وفي غير هذه الأحوال يحكم فقط بمصادرة القطع المرنة التي تم بها ارتكاب الجريمة وكان احرازها او حيازتها رقميا يشكل جريمة في ذاته.

مادة (71)
معاقبة الشخص الخطر في الجرائم الماسة بشخصية الدولة

فيما يتعلق بالوقائع التي تمس شخصية الدولة تطبق بشأن الشخص الخطر وفق أحكام هذا القانون أحكام المادة (135) وما بعدها من قانون العقوبات ولو لم يرتكب جريمة. ويتم التحفظ عليه لدى الجهات الأمنية المدة التي يقررها قاضي التحقيق.
ويتم انهاء حالة الخطورة بناء على تقرير الجهة الامنية إذا أمضى نصف المدة المحكوم بها على الاقل.
وللجهة الامنية تشغيل الشخص الخطر وفق هذا القانون فيما تراه مناسبا في هذا الشأن دون التزام عليها بتشريعات العمل والاستخدام والوظيفة العامة خلال المدة المحكوم بها.

مادة (72)
التدابير الامنية

يُعتد بالمناهج العلمية المتطورة في نظم أمن المعلومات فيما يتعلق بالإجراءات السابقة المتخذة لمكافحة حالة الخطورة المؤدية الى الجريمة الافتراضية، وذلك تحت اشراف عضو نيابة عامة. وتستمر تلك الاجراءات الى حين ثبوت انتهاء حالة الخطورة. ويجوز أن تكون تلك الاجراءات سرية او علنية حسب الاحوال.

مادة (73)
التدابير اللاحقة

تطبق النصوص المتعلقة بالتدابير الوقائية المقررة في قانون العقوبات على حالة الخطورة الرقمية وبالقدر الذي يبرر وجودها قاضي الموضوع دون اعتداد بالمدد المقررة في تلك النصوص.

مادة (74)
الاحالة على التشريع التقليدي

إذا وجد نص في هذا القانون يقرر الاحالة على قانون آخر في تقرير عقوبة معينة ذات حد أدنى او أقصى يراعى دائما أخذ الحد الأدنى في الاعتبار ما لم تكن الجريمة من احد الجرائم التالية:

- **الجرائم الماسة بشخصية الدولة.**
- **جرائم العدوان على الملكية الفكرية.**
- **جرائم العدوان على حرمة الحياة الخاصة.**

الباب الثالث
القاعدة الاجرائية

مادة (75)
أحكام عامة

تسري قواعد القانون الاجرائي التقليدية فيما لم يرد به نص في هذا القانون.

الفصل الأول
الاختصاص القضائي

مادة (76)
اختصاص القضاء الليبي

تطبق قواعد الاختصاص التقليدية في كل جريمة من الجرائم المنصوص عليها في هذا القانون والتي ترتكب في القطر الليبي، ويراعى في تطبيق هذا النص:

- **المادة (189- الفقرة الثانية) من قانون العقوبات.**
- **المصلحة الاجتماعية الاقتصادية للدولة الليبية.**
- **الاتفاقيات الدولية التي تبرمها ليبيا او تكون طرفا. وليس لقاضي الموضوع تجاوز النصوص الواردة في هذا القانون وتطبيق نصوص الاتفاقية ما لم يكن قرار الاحالة من النيابة العامة مبنيا على هذا الاساس.**

مادة (77)
المواقع الايجابية والسلبية

يراعى في اختصاص القضاء الليبي منطق الحركة الرقمية وتأثير المواقع الايجابية والسلبية المستخدم في تصميم المواقع عبر الانترنت.

مادة (78)
الاحالة على التشريع الاجرائي التقليدي

إذا وجد في هذا القانون ما يجيز الاحالة الى تشريع اجرائي تقليدي فإنه يراعى تنفيذ النص التقليدي إذا كان يتميز بحقوق أكثر للمتهم عما عليه الحال عند تطبيق نصوص هذا القانون.

الفصل الثاني
الاثبات الرقمي

مادة (79)
مدة ضبط والتحفظ على الحواسيب

فيما خلا الجرائم الماسة بشخصية الدولة او الجرائم التي يجوز فيها المصادرة فإنه لا يجوز بأي حال من الاحوال استمرار ضبط والتحفظ على الحواسيب والقطع الصلبة والمرنة بقصد اجراء فحص او تفتيش فيها بحثا عن جريمة لمدة تجاوز ثلاثة شهور، ويترتب البطلان على مخالفة هذه المادة.

مادة (80)
التفتيش الرقمي

لا يجوز التفويض في اصدار أذن التفتيش تنفيذا لهذا القانون، ولا يجوز اصدار أذن تفتيش عام ما لم يكن التفتيش مقررا بشكل رقمي. وفي هذه الحالة يجب النص في أذن التفتيش على الغاية منه بشكل واضح وصريح ومباشر وبحيث يشتمل أيضا على تحديد المسار الذي يتم من خلاله التفتيش الرقمي.

ويعد التفتيش رقميا إذا تم باستخدام النظام التراسلي فقط وبما يستدعي ذلك تتبع حركة مرتكب الجريمة عبر الخوادم والمضيفات بقصد الوصول الى الحاسوب الذي انطلق منه النشاط التقني في الجريمة.

مادة (81)
مراقبة مسار او حركة البيانات

يجوز تحت اشراف قاضي التحقيق مراقبة النظام التراسلي والشبكات والحواسيب المشتركة ومزودي الخدمات بقصد التوصل الى الجريمة ومرتكبها. ويصدر قاضي التحقيق أذنا بالمراقبة بعد سماع أقوال ممثل الجهة القائمة بالمراقبة. ويجوز الاستعانة بخبير او استشاري لأداء مهمة المراقبة. وفي هذه الحالة يتولى الخبير او الاستشاري القيام بالمراقبة تحت اشراف قاضي التحقيق مباشرة.

ويجوز في حالة الاستعجال الاعتداد بمحضر ضبط حركة او مسار البيانات. وتعد حالة الاستعجال هنا في مرتبة التلبس. ويلزم في هذه الحالة عرض محضر الضبط فورا على قاضي التحقيق لاستصدار امر باستمرار السير في الاجراءات او استصدار امر بالا وجه لإقامة الدعوى.
ولا يجوز مباشرة الدعوى او الاستمرار فيها إذا لم يتضمن ملف الدعوى تقريرا تقنيا مفصلا لهذه المراقبة المسبقة التي اسفرت عن الكشف عن الجريمة ومرتكبها. ويجوز للسلطات التقرير بسرية تقنية او غيرها تم استخدامها في المراقبة وعدم الكشف عنها في المحكمة.

مادة (82)
التتبع المادي للخوادم والمضيفات

يُكتفى بأذن تفتيش واحد إذا كان هناك دلالة تستدعي تتبع مسار الجريمة بالانتقال المادي بين الخوادم في أماكن مختلفة.
ولا تسري هذه المادة إذا كان بين هذه الأماكن حواسيب او خوادم في مساكن خاصة.
ويراعى مبدأ التعاون الدولي والثنائي والإنابة القضائية في إطار التفتيش خارج الحدود الليبية إذا كان لذلك حاجة.

مادة (83)
استخلاص الدليل من حاسوب المجني عليه

ليس في هذا القانون ما يبرر تفتيش حاسوب المجني عليه. وعلى استثناء يجوز تفتيش حاسوب المجني إذا كان هو السبيل الوحيد لاستخلاص الدليل وقبل هو ذلك كتابة في محضر رسمي.

مادة (84)
ضبط وتفتيش حاسوب الجاني

يجوز اتخاذ اجراءات مادية لضبط حاسوب الجاني دون المساس بحقوقه التي يقررها القانون.
ويلزم التحفظ على حاسوب الجاني بطريقة تسمح باستخدام النظم المتطورة في التفتيش التقني.
وتتم مباشرة اجراءات تفتيش حاسوب الجاني من قبل خبرة متخصصة محلفة. وفيما عدا الجرائم المرتكبة ضد أمن الدولة وشخصيتها فإنه ليس في هذا القانون ما يبرر التحفظ على القطع الصلبة لحاسوب الجاني لأكثر من ثلاثة شهور.

مادة (85)
الشهادة الرقمية

أداء الشهادة رقميا مقبول في كافة الاحوال، سواء كانت الوقائع المنسوبة للمتهم مادية او رقمية.
ولو كان الشاهد خارج الحدود الاقليمية ما دام الشاهد يدلي بشهادته تحت اشراف قضائي ليبي أو أجنبي محلف، ويجب ان يتم تحليف من حضر الادلاء بالشهادة اليمين بأنه يقر بأن الشاهد الذي يدلي بشهادته هو المقصود وانه تعرف على شخصه وصفته وهويته وكذلك تكرار اقواله. وإذا كان

الشاهد صغيرا او عاجزا او في حالة الاستعجال يجوز ان تكون الشهادة مسجلة رقميا وفي غير الزمن الفعلي لها شريطة ان تكون ثابتة التاريخ.

مادة (86)
الغاية من التفتيش

ليس في هذا القانون ما يبرر الخروج على المادة (39) من قانون الاجراءات الجنائية. ومع ذلك فإن اكتشاف جريمة ما بطريق الصدفة يبرر اتخاذ اجراء التحفظ الى حين اتخاذ الاجراءات الجنائية. ويجوز لكل انسان اتخاذ اجراءات التحفظ المذكورة شريطة ابلاغ السلطات خلال مدة معقولة.

مادة (87)
حماية الشهود

يجوز وضع برامج أمنية لحماية الشهود. وإذا كان الشاهد صغير السن يجوز الاكتفاء بسماع شهادته او الحصول على شهادته مسجلة او الادلاء بها رقميا دون لزوم حضوره مع الاحتفاظ بسرية شخصيته.

مادة (88)
ضبط الجريمة العرضية

يراعى في تفتيش حاسوب او شبكة او خادم او مضيف الجاني المادة (39) من قانون الاجراءات الجنائية. ولا تطبق هذه المادة في الاحوال التالية:

- الجرائم الماسة بشخصية الدولة.
- الجرائم الاخلاقية.
- الجرائم الدولية او ذات الطابع الدولي.

الفصل الثالث
الخبرة التدريبية والتقنية

مادة (89)
الخبرة التدريبية

الخبرة التدريبية في مجال الحوسبة والرقمية عنصر رئيسي في تكوين قناعة قاضي الدعوى إذا رأى وجها لذلك وفي أي مرحلة من مراحل الاجراءات ولو كانت الدعوى امام المحكمة العليا.

مادة (90)
اليمين التدريبية

يجوز لقاضي الموضوع او لعضو التحقيق ايقاف اجراءات الدعوى لمدة معقولة واستحضار خبير تدريبي متخصص ومحلف وذلك للاستعانة به في تطوير أدائه القانوني والتقني في مسألة او أكثر تتعلق بسير الدعوى. وفي هذه الحالة يحيل القاضي او عضو هيئة التحقيق مصاريف التدريب على رئيس المحكمة.
ويجب أن تتضمن اليمين التدريبية للخبير أنه على دراية بآخر المستجدات التقنية والتطوير الذي وصلت اليه الحوسبة والرقمية.

الفصل الرابع
الارشاد الرقمي

مادة (91)
أوراق المحضرين رقميا

في إطار تنفيذ هذا القانون، تكون أوراق المحضرين التي يتم تبليغها رقميا ذات القيمة القانونية لأوراق المحضرين التقليدية وتتساوى معها. ويتم التبليغ وفق الاجراءات التي يحددها وزير العدل.

مادة (92)
البلاغ الرقمي

تكون الجهة المختصة مسئولة عن عدم الالتزام بالاستدلال في كل بلاغ رقمي يصل اليها.
ويعاقب المسئول عن استلام البلاغات بالعقوبات المقررة في قانون العقوبات عن كل اهمال في الاهتمام بالبلاغ الرقمي. وتطبق في شأن المبلغ أحكام جريمة الافتراء والبلاغ الكاذب المقررة في قانون العقوبات إذا ثبت أن بلاغه غير صحيح.
ويعفى المبلغ من العقاب إذا كان أساس بلاغه توقع معقول وفقا للظروف العادية وبمعيار الرجل المتوسط او العادي.

مادة (93)
نظم الاستعارة السرية

يجوز لرجال الضبط القضائي تطبيق نظم الاستعارة السرية ولمدة محدودة، وذلك تحت اشراف قاضي الامور الوقتية او قاضي الموضوع حسب الاحوال وذلك بقصد الكشف عن الجرائم ومرتكبيها.

مادة (94)
اثبات السب والقذف والتشهير والتهديد

يُكتفى في تحريك ورفع الدعوى الجنائية في جرائم السب والقذف والتشهير والتهديد وفقا للمواد (41- 42- 43- 44) من هذا القانون قيام المتضرر من الجريمة بتقديم النسخة الرقمية ولو كانت في هيئة مطبوعة. وفي حالة الانكار تسري القواعد العامة المقرر في هذا القانون دون غيرها.

ملحق
القرارات المنفذة للقانون

دولة ليبيا
مجلس الوزراء

قرار رقم..... لسنة.....
بشأن تشكيل لجنة متابعة قانون الجريمة الافتراضية والدليل الرقمي

مجلس الوزراء
بعد الاطلاع على،
قانون اصدار القانون رقم..... لسنة..... بشأن الجريمة الافتراضية والدليل الرقمي.

مادة ()
تشكل لجنة تسمى لجنة متابعة قانون الجريمة الافتراضية والدليل الرقمي ذات استقلال مالي واداري وتتبع نوعيا رئيس مجلس الوزراء، أعضاؤها من الاخوة والاخوات التالية أسمائهم:
- **الاخ**
-

مادة ()
تكون المهام الموكولة للجنة المذكورة على النحو التالي:
1- **مراقبة قيام مختلف السلطات بتنفيذ قانون الجريمة الافتراضية.**
2- **البحث المستمر في عملية تطوير قانون الجريمة الافتراضية والدليل الرقمي.**
3- **رصد الدراسات والبحوث والتقارير والتفسيرات الخاصة التي ترد حين تنفيذ هذا القانون وتحضير المذكرات الايضاحية للتعديلات التي قد تعرض له.**
4- **الاتصال الدولي والمحلي بالجهات والباحثين في مجال الجريمة الافتراضية والدليل الرقمي والتعاون معهم بهدف البحث عن الحلول التي تطرحها المشكلات الجديدة والتطوير المستمر.**
5- **نشر الدراسات والبحوث واعداد الانشطة المختلفة والمؤتمرات والمشاركة فيها على المسنوى الدولي والمحلي.**
6- **وضع الفتاوي القانونية والاقتصادية وتقرير التفسيرات الدقيقة والاستشارات التي ترد اليها من الجهات المختلفة حول القانون.**

مادة ( )
ينشر هذا القرار في الجريدة الرسمية ويعمل به من تاريخ نشره.

مجلس الوزراء

وزير الداخلية
قرار وزير الدخلية رقم ( ) لسنة .....
بشأن تطبيق المادة 27 من قانون الجريمة الافتراضية

وزير الداخلية،
بعد الاطلاع على،
القانون رقم..... لسنة..... بشأن الجريمة الافتراضية والدليل الرقمي.
والقرار رقم.... لسنة..... بشأن انشاء مكتب مكافحة جرائم الانترنت.
والقرار رقم..... لسنة.....
وبناء على ما عرضته لجنة متابعة قانون الجريمة الافتراضية المشكلة وفق قرار مجلس الوزراء رقم..... لسنة.....

قرر

مادة ( )

يلتزم مزودو الخدمة والاستضافة باستخدام أساليب تقنية مناسبة بهدف المحافظة على المخزون الرقمي والمعلوماتي في تلك المضيفات وبحيث تتحمل قدرات التخزين في المزودات المدد المحددة في هذا القرار.

مادة ( )

يكون الحد الادنى للمدة اللازمة للتحفظ والاستضافة المقررة في المادة (27) من قانون الجريمة الافتراضية تسعين يوما. واما حدها الاقصى سنة ميلادية كاملة.

مادة ( )

1- يلتزم مزودو الخدمة والاستضافة بمسك دفاتر التحفظ والاستضافة ويدون فيها تسجيل دقيق وبخط واضح تواريخ ازالة التحفظ والاستضافة في المدد اللازمة لذلك. ويتم ختم صفحات هذه الدفاتر من قبل المكتب المختص في الوزراة.
2- يلتزم مزودو الخدمة والاستضافة عند القيام بانهاء حالة التخفظ والاستضافة خلال المدة اللازمة لذلك بتقديم طلب للمكتب المختص في الامانة للموافقة على انهاء حالة التخزين.
3- لمباشرة عملية انهاء التخزين يجب أن يكون ذلك بعد صدور موافقة على الطلب المبين في الفقرة السابقة.
4- يلتزم مزودو الخدمة والاستضافة بتجهيز الشبكات بآليات وتقنيات مناسبة لتنفيذ هذا القرار.

مادة ( )

يفصل المكتب المختص في الطلب خلال ثمان وأربعين ساعة. وفي حالة رفض الطلب يعاد تقديمه بعد ثلاثة أشهر. وفي كل الاحوال لا يجوز استمرار رفض الطلب لمدة تزيد عن سنة. فإذا مضت مدة السنة يجوز لمزود الخدمة والاستضافة ازالة التخزين بعد تقديم مذكرة الى المكتب المختص تتضمن فوات مدة سنة دون انتظار للفصل في المذكرة.

مادة ( )

ينشر هذا القرار في الجريدة الرسمية ويعمل به من تاريخ نشره.

وزير الداخلية

دولة ليبيا
وزير العدل

قرار وزير العدل رقم..... لسنة.....
بشأن استخلاص وحفظ الادلة الرقمية

وزير العدل،
بعد الاطلاع على،
المواد (27- 29- 70- 79- 84) من قانون الجريمة الافتراضية،
و

قرر
مادة (1)
يتم حفظ الأدلة الرقمية تحت اشراف النيابة العامة وبمعرفة خبير من المعامل الشرعية في القضايا الجنائية. وفيما خلا الجرائم المنصوص عليها في المادة (79) من قانون الجريمة الافتراضية فإنه لا يجوز أن تزيد مدة الضبط والتحفظ على الحواسيب عن تسعين يوم عمل رسمي. على أن يتم حساب المدة المذكورة بساعات العمل وليس بالايام (اليوم= عدد اربعة وعشرين ساعة عمل= اربعة ايام تقليدية).

مادة ()
يجوز الاستعانة بخبرة خارجية محلفة تتولى اعمال استخلاص والتحفظ على الدليل الرقمي وفي هذه الحالة يجب أن يكون الخبير مؤهلا بالتقنيات الحديثة ومعترفا به كمكتب او مركز متخصص. ويلتزم بالالتزامات المقررة في اطار سرية التحقيق في قانون الاجراءات الجنائية. وتسري عليه احكام المادة (4/16) من قانون العقوبات لسنة 1953.

مادة ()
يجوز للخبراء والمحامون والاستشاريون القانونيون والعاملون في مجال المساعدة القانونية وخبراء الحوسبة والرقمية فتح مكاتب معترف بها من وزارة العدل يكون مهمتها الدليل الرقمي.

مادة ()
يكون فتح المكاتب المشار اليها في المادة السابقة بناء على طلب يقدم الى الامانة يتضمن الاوراق التالي:

1- **طلب.**
2- **شهادات الخبرة اللازمة.**
3- **شهادة من ثلاثة خبراء حوسبة ورقمية محلفين مبين فيها حداثة او تحديث الحواسيب والالات المستخدمة في استخلاص وفحص وحفظ الادلة الرقمية.**
4- **تراخيص حيازة حواسيب استخلاص وفحص وحفظ الادلة الرقمية.**

5- اسم الخبير المتخصص الذي يتم الاستعانة به في المكتب.
6- ما يفيد حيازة القطع الصلبة والمرنة والتراخيص اللازمة لذلك.
7- دلالة على المكان الذي يتم فيه مباشرة العمل (عقد ايجار- اوراق ملكية-..الخ).
8- شهادة من شركة تأمين شاملة لمكان مباشرة العمل.

مادة ()
يصدر تعميم عن وزارة العدل فيما يتعلق بضرورة تحديث حواسيب استخلاص وفحص وحفظ الادلة الرقمية.

مادة ()
ينشر هذا القرار في الجريدة الرسمية ويعمل به من تاريخ نشره.

وزير العدل

دولة ليبيا
وزارة العدل

قرار وزير العدل رقم..... لسنة.....
بشأن أوراق المحضرين رقميا

وزير العدل،
بعد الاطلاع على،
المواد (35- 91) من قانون الجريمة الافتراضية،
قرر
مادة ()
في اطار تنفيذ قانون الجريمة الافتراضية والدليل الرقمي، يكون تبليغا صحيحا قيام قلم المحضرين باستخدام البدائل المختلفة للحوسبة والرقمية لتبليغ الاشخاص بمحتوى أوراق المحضرين. ويكون لقوة تبليغ المحتوى ذات القيمة القانونية لاستلام الأوراق الرسمية المعلنة عن طريق المحضرين، وعلى مستلم ورقة المحضرين اثبات عدم استلامه اوعلمه لذلك حسب الاحوال.
مادة ()
ينشر هذا القرار في الجريدة الرسمية ويعمل به من تاريخ نشره.

وزير العدل

دولة ليبيا
وزارة الاعلام والثقافة
بتنظيم موضوع قيام الافراد والمؤسسات بتنظيم الجوائز باستخدام خوادم ليبية او على الليبيين.

وزير الاعلام والثقافة،

بعد الاطلاع على المادة (49) من قانون الجريمة الافتراضية والدليل الرقمي،

مادة ()
يختص مدير ادارة الاعلام الالكتروني بالوزارة باصدار الموافقات على طلبات معدي الجوائز واللوتريا باستخدام الحوسبة والرقمية والانترنت وبأي قيمة كانت. ولا يسري هذا القرار على الجوائز التي تتم باستخدام وسائل الاتصالات.

مادة ()
تشكل لجنة برئاسة مدير الادارة المذكورة وعضوية مستشار قانوني ومالي وعضو عن منظمة أهلية ذات مصلحة في تطبيق هذا القانون وذلك لتحديد وضبط معايير الجوائز عبر الانترنت. ويسود نظام الاغلبية التصويت في هذه اللجنة على القرارات مع مراعاة ان صوت الرئيس صوتان في حالة تساوي الاصوات.

ويحكم عمل هذه اللجنة مباديء الادارة الرشيدة وقواعد الشفافية.
ويكون من اختصاص هذه اللجنة النظر في أية منازعات قد تنشأ في اطار تلك الجوائز. ويكون حكمها بمثابة قرار اداري واجب التنفيذ ما لم يتم الطعن عليه خلال المدة المقررة للطعن على القرارات الادرية. وفي حالة وجود شبهة جنائية تحيل اللجنة المختصة ملف النزاع الى النيابة العامة فورا ودون تأخير. ويترتب على التأخير في هذه الحالة عدم سريان مدة التقادم المقررة.

مادة ()
ينشر هذا القرار في الجريدة الرسمية ويعمل به من تاريخ نشره.

وزير الاعلام والثقافة

ضيف وحوار

الدكتور بوغرارة محمد الفرجاني
أول من أدخل قانون الإنترنت إلى الدراسات الأمنية العليا

بوابة القانون في العالم الرقمي

- **دكتور بوغرارة، بداية نرحب بك في مجلة البوصلة الرقمية، ويسعدنا أن تكون ضيف هذا العدد، نود أن نبدأ بالتعريف بمسيرتك الأكاديمية والمهنية باختصار.**

شكرًا لمجلتكم على هذا اللقاء. أنا الدكتور بوغرارة الفرجاني، أستاذ القانون الدولي، عملت طويلًا في مجالات التشريع والبحث الأكاديمي، وأسهمت في تطوير مناهج دراسات عليا متعددة، من أبرزها منهج "قانون الإنترنت"، الذي كان ثمرة رؤية استراتيجية لمواكبة التحولات الرقمية وأثرها على البنية القانونية والأمنية للدول. وكذلك دبلوم ادارة الازمات والكوارث.

- **ما هي الدوافع والمبررات التي دفعتكم لإدخال "قانون الإنترنت" كمقرر أكاديمي ضمن كلية الدراسات العليا للعلوم الأمنية؟**

في ظل التحول الرقمي المتسارع، أصبح العالم الرقمي مساحة جديدة للجريمة والتهديدات. لاحظنا فجوة خطيرة بين التكوين الأمني التقليدي وواقع الجرائم الإلكترونية، ما تطلب تدخلًا عاجلًا. كان إدخال منهج "قانون الإنترنت" ضرورة ملحة لتمكين الضباط والدارسين من أدوات قانونية وتحليلية لفهم البيئة الرقمية، والتعامل مع الجرائم السيبرانية والتقنيات الجديدة، ضمن إطار قانوني واضح.

- **كيف كانت ردود الأفعال الأكاديمية والإدارية على هذه المبادرة الجريئة؟ وهل واجهتم تحديات؟**

كما هو متوقع، واجهنا في البداية شيئًا من التردد، لأن الموضوع جديد ومعقد. ولكن سرعان ما تبدلت المواقف بعد تقديم تصور علمي متكامل مدعوم بالأمثلة والإحصائيات. حصلنا على دعم إداري من عمادة الكلية، وتعاون أكاديمي مثمر، خاصة مع تنامي الوعي بخطورة الجرائم الرقمية، مما شجع على دمج المقرر ضمن الخطة الدراسية.

- **كيف استُقبل هذا المنهج من قبل الطلاب؟ وهل لاحظتم تغييرًا في وعيهم القانوني تجاه الجريمة الرقمية؟**

كانت الاستجابة من الطلاب مذهلة. وُجد شغف حقيقي لديهم لمعرفة كيفية عمل القانون في عالم الإنترنت. طرحوا أسئلة عميقة حول الخصوصية، والاختراقات، والأدلة الرقمية. المنهج فتح أمامهم آفاقًا جديدة لفهم

الجريمة الرقمية ليس فقط من زاوية أمنية، بل من منظور قانوني وتشريعي شامل وخاصة كان للمشرفين علي تدرس هذا المقرر كل من **الدكتور محمد حسين الدكتور عمر بن يونس**:

- **هل ظهرت نتائج ملموسة لهذا المنهج في الواقع الأمني أو التشريعي؟**

بكل تأكيد. عدد من خريجي هذا البرنامج باتوا يشغلون مواقع قيادية في وحدات مكافحة الجرائم الإلكترونية. بعضهم شارك في إعداد لوائح وقوانين رقمية ومنهم **المستشار فرج برنوص**. وأصبح لدى الكلية اليوم نواة فكرية متقدمة في فهم تحديات الإنترنت من منظور أمني وقانوني، مما يعزز الأمن الوطني في وجه التهديدات السيبرانية.

- **كلمة أخيرة توجهونها للقراء والباحثين في مجال القانون الرقمي؟**

العالم يتغير، والقانون يجب أن يواكبه لا أن يتأخر عنه. أنصح الباحثين والمشرعين بأن يفتحوا أعينهم على التحديات القادمة: الذكاء الاصطناعي، العملات الرقمية، الواقع الافتراضي... كلها قضايا قانونية بامتياز. إذا لم نكن جاهزين، سندفع الثمن.

في الختام:

نتوجه بالشكر والتقدير للدكتور بوغرارة البوعيشي على هذا اللقاء الغني والمُلهم، ونتطلع إلى رؤية مبادراته القادمة في تعزيز التشريع الرقمي ضمن المنظومة القانونية والأمنية والى لقاء اخر مع شخصية مبادرة او ملهمة في مجال العالم الافتراضي؟

شروط النشر في المجلة القانونية

1. القيمة القانونية

يُشترط أن يكون العمل ذا قيمة قانونية، ويتناول مواضيع مهمة ومتطورة في الجانبين القانوني والقضائي.

2. المنهجية العلمية

يجب أن يكون البحث المُحكَّم متوافقًا مع الأصول العلمية الصحيحة والمعايير الأكاديمية المعتمدة.

3. طريقة التقديم

* يُقدَّم العمل مطبوعًا على قرص مدمج (CD) باستخدام خط عربي بحجم 14، أو يُرسل عبر البريد الإلكتروني الخاص بالمجلة.

* يجب مراعاة التدقيق اللغوي والإملائي قبل التقديم.

4. عدد الكلمات والصفحات

* يجب ألا يقل عدد كلمات البحث المُحكَّم عن 5000 كلمة، وألا يزيد عن 12,000 كلمة.

* يتراوح عدد الصفحات بين 12 إلى 30 صفحة.

5. عملية التقييم

* تخضع البحوث المُحكَّمة لتقييم الهيئة الاستشارية العلمية، وفقًا للأصول العلمية.

* تخضع الأعمال الأخرى (مثل المقالات أو التراجم) لتقييم هيئة التحرير.

6. مسؤولية الآراء

الأبحاث والمقالات والتراجم المنشورة في المجلة لا تعبّر عن رأي أو توجه المجلة، وإنما تعبّر عن آراء أصحابها فقط.

7. عدم استرجاع الأبحاث

جميع الأبحاث والمقالات والتراجم المقدمة لا تُعاد إلى أصحابها، سواء تم نشرها أم لم تُنشر.

8. السيرة الذاتية

يجب أن يُرفق مقدّم العمل نبذة موجزة عن سيرته الذاتية، تتضمن المؤهلات والخبرة العلمية.

للتواصل وإرسال الأعمال

* الهاتف: +218 93 482 5045

*البريد الإلكتروني: bawsala@cid.gov.ly

مجلة
البوصلة الرقمية

المجلة الليبية لقانون الانترنت

تصدر عن إدارة مكافحة جرائم تقنية المعلومات
جهاز المباحث الجنائية / وزارة الداخلية الليبية

تمت طباعة هذا العدد بمساهمة من شركة الود للتدريب و الاستشارات