جامعة النجاح الوطنية
كلية الدراسات العليا

الاعتداءات الالكترونية الواقعة على الامن الداخلي للدولة ودور اجهزة العدالة في مكافحتها

إعداد
أسيل أيمن "محمد كمال" البكري

إشراف
د. فادي شديد
د. عبدالله محمود السفاريني

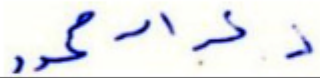
قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في القانون الجنائي من كلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين.
2025

الاعتداءات الالكترونية الواقعة على الامن الداخلي للدولة ودور اجهزة العدالة في مكافحتها

إعداد

أسيل أيمن "محمد كمال" البكري

نوقشت هذه الرسالة بتاريخ 2025/12/18م، وأجيزت:

د. فادي شديد	
المشرف الرئيسي	**التوقيع**
د. عبدالله محمود السفاريني	
المشرف الثاني	**التوقيع**
د. غسان عليان	
الممتحن الخارجي	**التوقيع**
د. نور عدس	
الممتحن الداخلي	**التوقيع**

الإهداء

الى دماء شهداء فلسطين التي روت أرضنا وما زالت

الى القابعين خلف القضبان... الى اسرانا البواسل

الى الذي أفنى عمره لأجلي، الى من غرس في قلبي عزيمة لا تلين... والدي الحبيب

الى من أغدقت عليّ الحب والدعم في كل لحظة، الى التي لا تطيب الحياة الا بها... أمي الغالية

الى اخوتي سندي وعضدي

اهدي ثمرة جهدي

الإقرار

أنا الموقعة أدناه مقدمة الرسالة التي تحمل عنوان:

الاعتداءات الالكترونية الواقعة على الامن الداخلي للدولة ودور اجهزة العدالة في مكافحتها

أقر بأن ما اشتملت عليه هذه الرسالة هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة اليه حيثما ورد، وأن هذه الرســـالة ككل أو أي جزء منها لم يقدم من قبل لنيل أية درجة أو لقب علمي أو بحثي لدى أية مؤسسة تعليمية أو بحثية أخرى.

اسم الطالبة: **أسيل أيمن "محمد كمال" البكري**

التوقيع: أسيل البكري

التاريخ: **2025/12/18**

فهرس المحتويات

الإهداء ..... ج

الإقرار ..... د

فهرس المحتويات ..... هـ

الملخص ..... ز

المقدمة 1

اشكالية الدراسة 2

أهمية الدراسة 3

أهداف الدراسة 4

منهجية الدراسة 5

الدراسات السابقة 5

الفصل الأول: ماهية الاعتداءات الالكترونية على الامن الداخلي للدولة 9

المبحث الأول: المقصود بالاعتداءات الالكترونية والامن الداخلي للدولة 10

المطلب الأول: الطبيعة القانونية للاعتداء الالكتروني 11

المطلب الثاني: التعريف بالأمن الداخلي للدولة والأمن المعلوماتي 17

المبحث الثاني: صور الاعتداءات الالكترونية على أمن الدولة الداخلي 21

المطلب الأول: التحريض على الفتنة الداخلية عبر الوسائط الإلكترونية 22

المطلب الثاني: نشر معلومات كاذبة تؤثر على الرأي العام 27

المطلب الثالث: التلاعب في البيانات الحكومية الحساسة 36

المطلب الرابع: الارهاب الالكتروني وصوره 43

الفرع الاول: انشاء مواقع الكترونية إرهابية 47

الفرع الثاني: تدمير المواقع والبيانات والأنظمة الالكترونية 49

الفرع الثالث: التهديد والترويع الالكتروني 53

الفرع الرابع: تمويل الارهاب عبر شبكة الانترنت 53

الفرع الخامس: التجسس الالكتروني لصالح الجماعات الإرهابية 57

الفصل الثاني: دور اجهزة العدالة في مكافحة الاعتداءات الالكترونية على امن الدولة الداخلي 59
المبحث الاول: الدور القانوني والتنظيمي للأجهزة في فلسطين 60
المطلب الأول: دور الشرطة ووحدة الجرائم الإلكترونية 63
الفرع الأول: آلية تلقي البلاغات الالكترونية 64
الفرع الثاني: التحقيقات الرقمية ووسائل الإثبات 65
الفرع الثالث: التحديات التي تواجه الوحدة 65
المطلب الثاني: دور الجهاز الوقائي الفلسطيني في الاعتداءات الالكترونية على أمن الدولة الداخلي ... 66
الفرع الأول: الرقابة على الانترنت ضمن القانون 68
الفرع الثاني: كشف الشبكات الداخلية والخارجية 69
الفرع الثالث: التحديات القانونية واللوجستية 70
المبحث الثاني: تحليل الإجراءات المتبعة في المكافحة 71
المطلب الأول: إجراءات مستحدثة لمكافحة الاعتداءات الإلكترونية في التشريع الفلسطيني..... 71
الفرع الأول: التفتيش الإلكتروني..... 72
الفرع الثاني: الحصول على المعلومات من مزودي الخدمة 75
الفرع الثالث: الاعتراض الالكتروني من قبل الجهات المختصة 76
الفرع الرابع: حجب المواقع الالكترونية 78
المطلب الثاني: إجراءات حديثة لمكافحة الاعتداءات الإلكترونية لم يتناولها المشرع الفلسطيني..... 79
الفرع الاول: التحليل الاستخباري للبيانات الرقمية 80
الفرع الثاني: التعاون بين القطاعين الأمني والتقني 82
الخاتمة 85
النتائج 85
التوصيات 87
المراجع العلمية 88
Abstract ..... b

الاعتداءات الالكترونية الواقعة على الامن الداخلي للدولة ودور اجهزة العدالة في مكافحتها

إعداد

أسيل أيمن "محمد كمال" البكري

إشراف

د. فادي شديد

د. عبدالله محمود السفاريني

الملخص

تعالج هذه الدراسة موضوع الاعتداءات الإلكترونية على أمن الدولة الداخلي في فلسطين، باعتبارها من القضايا المستحدثة التي تمثل تحدياً متزايداً للمشرع وللجهات المختصة على حد سواء في ضوء التطورات التقنية المتسارعة. فمع تزايد الاعتماد على مثل هذه التقنيات في مختلف المجالات، ساهم ذلك في ظهور اشكال جديدة من الجرائم التي تستهدف البنى التحتية للمعلومات، والمواقع الحكومية وهو ما ينعكس بصورة مباشرة على استقرار الدول وأمن المجتمعات.

ان هذه الدراسة تهدف الى توضيح الاعتداءات الأمنية الالكترونية التي قد تقع على امن الدولة الداخلي من خلال الشبكة العنكبوتية، حيث ان اشكالية الدراسة تتمحور بشكل اساسي حول مدى كفاية الإطار القانوني المنظم لهذه الجرائم في ضوء التشريعات الفلسطينية، والى أي مدى تسهم أجهزة العدالة في مكافحة الاعتداءات الالكترونية الماسة بأمن الدولة الداخلي، مع بيان أوجه القصور في التشريع الجزائي الفلسطيني من خلال مقارنته بالتجارب العربية الأخرى للاستفادة منها.

وخلصت هذه الدراسة الى أن حماية أمن الدولة الداخلي في ظل الفضاء الالكتروني تتطلب تحديثاً للنصوص الناظمة للجرائم الالكترونية في فلسطين بما يواكب التطورات التقنية، وتعزيز قدرات الأجهزة الأمنية المختصة وتجهيزها بأدوات التحقيق الرقمي المتقدمة. كما تتطلب مكافحة الاعتداءات الالكترونية تطوير إجراءات

عملية وتقنية تتناسب مع طبيعتها وتعقيدها بما يضمن سرعة الاستجابة، ودقة جمع الأدلة وبالتالي تعزيز قدرة المنظومة الأمنية على مواجهة هذه الجرائم وحماية استقرار الدولة والمجتمع.

الكلمات المفتاحية: الاعتداءات الإلكترونية، أمن الدولة الداخلي، قانون الجرائم الالكترونية.

المقدمة

لقد ادى حجم التطور الهائل الذي شهدته شبكة المعلومات والانفتاح غير المحكوم جغرافياً الى تطور غير مسبوق في مختلف النواحي الاقتصادية والاجتماعية والثقافية والسياسية حيث اصبحت تعتمد بشكل اساسي على هذه الانظمة لما توفره من سرعة ودقة في الانجاز وتجميع المعلومات ومعالجتها وتخزينها، فأصبح تفاعل العالم المادي مع العالم الافتراضي سمة من سمات المجتمع المعاصر.

الا ان هذا لم يمنع من ظهور تحديات وتهديدات تواجه المجتمع وامنه جراء وجود من يسيء استخدام هذه الشبكة، فاستخدام هذه التكنولوجيا وشبكة الانترنت لم يقتصر فقط على الجانب الايجابي بل له مظاهر خطيرة سلبية أثرت على المجتمعات والدول و يظهر ذلك من خلال قيام بعض الافراد والجماعات باستغلال هذه المزايا في اغراض خطيرة، الامر الذي عكس الجانب السلبي للتطور الالكتروني، وهذا بدوره ادى الى بروز مجموعة من الجرائم المستحدثة التي تعتمد على اساليب متطورة، حيث تكون في بعض الاحيان اشد خطورة من الجريمة التقليدية، فمن سمات الجرائم التي تتم عن طريق الشبكة انها سهلة التنفيذ والتخفي، وذلك لما توفره الشبكة من قدرة على تدمير ومحو الادلة، حيث تعتبر شبكة المعلومات بيئة خصبة لارتكاب جرائم خطرة.

ولعل من اخطرها ما سنتناوله في دراستنا وهي الافعال الارهابية والتي اصبحت تتم بواسطة شبكة الانترنت، حيث ساهم التطور المعلوماتي بشكل كبير في تطوير اليات الارهاب لتشمل صور الكترونية تختلف عن تلك النمطية المتعارف عليها، وهذا ما جعل منها سلاحاً رهيباً و فتاكاً يستعمل لتفكيك الشعوب و زعزعة استقرار الدول و الأنظمة و الإطاحة بها، فلم يعد أي مجتمع من المجتمعات بمنأى عن هذه الظاهرة.

في السياق الفلسطيني، تبرز حساسية هذه الاعتداءات نظرًا للوضع السياسي والأمني الخاص، حيث إن البنية الأمنية الداخلية معرضة باستمرار لمحاولات الاختراق والتشويش عبر منصات التواصل الاجتماعي،

ووسائل الإعلام الرقمي، وغيرها من القنوات التقنية. ومع أن فلسطين أصدرت القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، فإن هذا القانون ركز بشكل أساسي على الجرائم المرتكبة ضد الأفراد أو المؤسسات من زاوية الحماية المدنية والجنائية، دون التوسع في معالجة الاعتداءات ذات الطابع السيادي أو المرتبطة بالأمن الداخلي للدولة بشكل شامل. يتضمن القانون مجموعة من المواد التي تُجرّم الدخول غير المشروع، وانتهاك الخصوصية، وتعطيل البيانات، ونشر محتوى غير مشروع عبر الوسائط الإلكترونية، وقد تم تعديله لاحقًا بالقرار بقانون رقم (38) لسنة 2021 لتوسيع نطاق التجريم، إلا أن كلا النصين ما زالا يفتقران إلى المعالجة الكاملة للأفعال التي تستهدف الأمن الوطني الرقمي أو تشكل تهديدًا سياسيًا ممنهجًا. لذلك، تبرز الحاجة إلى تطوير الإطار القانوني الحالي ليواكب التطور التكنولوجي، ويضع أدوات تشريعية واضحة لحماية السيادة الرقمية وملاحقة الفاعلين بشكل ناجع.

اشكالية الدراسة

تتمحور اشكالية الدراسة في التطور الهائل لأشكال الجرائم المرتبطة بتطور تكنولوجيا المعلومات والمتعلقة بالأمن الداخلي للدولة، حيث ساعد هذا التطور في سرعة تنفيذ هذا النوع من الجرائم وتعقيدها وتشابكها، وصعوبة حصرها في منطقة جغرافية محددة وبالتالي صعوبة اثباتها وملاحقة مرتكبيها.

فتتمثل اشكالية الدراسة بشكل اساسي حول مدى كفاية الإطار القانوني المنظم لهذه الجرائم في ضوء التشريعات الفلسطينية، والى أي مدى تسهم أجهزة العدالة في مكافحة الاعتداءات الالكترونية الماسة بأمن الدولة الداخلي؟

وتفرع عن هذه الإشكالية العديد من التساؤلات والتي ستقوم الباحثة بالإجابة عليها، وهي:

- ماهية الاعتداء الالكتروني على الامن الداخلي؟
- ما هو الامن الداخلي؟

- ما هو دور اجهزة الامن في ملاحقة مرتكبي هذه الجرائم؟
- ما هو الإطار التشـــريعي الذي ينظم مكافحة هذه الاعتداءات الالكترونية التي تمس امن الدولة الداخلي؟
- هل تعتبر النصـــوص القانونية المتعلقة بالجرائم الالكترونية كافية لمواجهة هذا النوع من الاعتداءات والحد منها؟
- هل الاجراءات الجنائية التقليدية تناسب طبيعة هذه الجرائم من حيث الملاحقة والتفتيش وجمع الادلة؟
- ما هي أبرز التحديات القانونية والفنية التي تعيق فعالية مكافحة الاعتداءات على أمن الدولة الداخلي؟

أهمية الدراسة

يكتسب موضوع هذه الدراسة اهمية متزايدة بسبب الاستغلال الكبير لوسائل الاتصال الحديثة في عصرنا الحالي من قبل مرتكبي الجرائم، والتي جعلت ارتكاب الجرائم من خلالها تتم بســـهولة وعن بعد، وكذلك سرعة الافلات لصعوبة تتبعهم.

فتكمن اهمية هذه الدراسة في انها تسلط الضوء على الافعال التي تشكل اعتداء على امن الدولة الداخلي وبشـــكل خاص جريمة الارهاب الالكتروني، حيث ان هذا النوع من الجرائم يهدف الى تدمير البنية التحتية المعلوماتية للدولة، وتهديد امنها والتي قد يكون الهدف من ذلك اجبار الحكومات والمجتمعات على افعال معينة لاغراض ســياســية او اجتماعية. كما وتكمن أهمية هذه الدراســة ايضــاً في محاولتها لبيان كيفية مواجهة الاعتداءات الالكترونية التي تقع على امن الدولة الداخلي في فلسطين، وفيما اذا تعتبر النصوص القانونية المتعلقة بالجرائم الالكترونية كافية للتصدي لهذه الاعتداءات.

الأهمية النظرية

تتمثل الأهمية النظرية لهذه الدراسة في أنها تسد فراغاً بحثياً في الدراسات القانونية الفلسطينية المتعلقة بأمن الدولة الداخلي في المجال الرقمي، فهي تسعى إلى اثراء الفقه القانوني الفلسطيني من خلال تناول موضوع مستجد يتمثل بالاعتداءات الإلكترونية الموجهة ضد الأمن الداخلي للدولة، والتي لم تدرج بشكل واضح في القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية أو تعديلاته. كما تسعى في بيان الإطار المفاهيمي والقانوني لهذه الاعتداءات وبيان موقعها ضمن منظومة الجرائم الماسة بأمن الدولة، بشكل يعزز من البناء النظري فيما يتعلق بالجرائم الالكترونية ويكشف مواطن الضعف في التشريع الفلسطيني مقارنة بالتشريعات العربية الأخرى التي تطرقت اليها في الدراسة.

الأهمية العملية

تتجلى الأهمية العملية لهذه الدراسة في انها تمثل إضافة للواقع القانوني الفلسطيني من خلال تسليط الضوء على الاعتداءات التي تقع على أمن الدولة الداخلي والنظام العام بطريقة إلكترونية، وابراز الحاجة الملحة الى تطوير المنظومة التشريعية في فلسطين لمواجهة هذه الاعتداءات، والتي يصعب التصدي لها بالأدوات التقليدية كونها تتسم بالحداثة وتنوع أساليب ارتكابها وسهولة افلات مرتكبيها من العقاب. فمن خلال التحليل المقارن، توفر الدراسة دعماً في صياغة نصوص أكثر دقة وشمولية، تراعي خصوصية الجرائم الالكترونية المرتبطة بالأمن الداخلي، كما وتقدم توصيات عملية يمكن ان يستفيد منها أجهزة العدالة وصانعي السياسات في مواجهة هذه الاعتداءات والمساهمة في تطوير التشريعات الخاصة بالجرائم الالكترونية والمتعلقة بأمن الدولة الداخلي.

أهداف الدراسة

تهدف هذه الدراسة الى:

1. تحديد الإطار المفاهيمي والقانوني للاعتداءات الالكترونية الماسة بأمن الدولة الداخلي في فلسطين.

2. تحليل النصوص القانونية المتعلقة بهذه الجرائم.

3. تسليط الضوء على المواجهة الجنائية والامنية لجرائم الارهاب الالكترونية.

4. بيان وتقييم دور جهاز الشـــرطة (وحدة الجرائم الالكترونية) في مواجهة الاعتداءات الالكترونية على امن الدولة الداخلي.

5. بيان دور الجهاز الوقائي الفلسطيني في مكافحة الاعتداءات الالكترونية.

6. البحث في التحديات والعقبات التي تواجه الأجهزة الأمنية الفلســـطينية في تعاملهم مع هذا النوع من الاعتداءات.

منهجية الدراسة

سـتعتمد هذه الدراسـة على المنهج الوصـفي الذي يقوم على وصـف الافعال التي تشـكل اعتداءً على امن الدولة والتطرق لظاهرة الارهاب الالكتروني والاثار الناجمة عنه، وكذلك طرق مكافحتها، والمنهج التحليلي الذي يقوم على شـرح وتحليل النصـوص القانونية التي تنظم هذه الافعال في فلسـطين. كما وتسـتند هذه الدراسة الى المنهج المقارن وذلك من أجل ابراز أوجه الشبه والاختلاف بين النماذج العربية، مما يساهم في تحديد نقاط القوة والضعف في التشريع الفلسطيني، وكذلك الاستفادة منها في المواضيع محل الدراسة.

الدراسات السابقة

رســـالة ماجســـتير بعنوان: جريمة الارهاب الالكتروني، توات عبد الحكيم، جامعة العربي التبســـي: تبسة/الجزائر، 2021.

سـعت هذه الدراسـة الى توضـيح مفهوم الارهاب الالكتروني وبيان دوافع واغراض الارهاب واركانه، وكذلك سـلطت الدراسـة الضـوء على الجهود المبذولة في مكافحة جريمة الارهاب الالكتروني سـواء على الصـعيد

الوطني (الجزائر) او الدولي والتعرف على اهم الوسائل والاساليب المعتمدة لدى الهيئات والمنظمات الدولية لمكافحة جرائم الارهاب الالكتروني.

رسالة ماجستير بعنوان: جريمة الاختراق السيبراني للأنظمة المعلوماتية الخاصة بمؤسسات الدولة وفق المرسوم بقانون اتحادي رقم (34) لسنة 2021، شما راشد الكندي، جامعة الشارقة: الامارات العربية المتحدة، 2021.

سعت هذه الدراسة الى توضيح ماهية جريمة الاختراق السيبراني للأنظمة المعلوماتية الحكومية، وبيان أركانها وما مدى فعالية قواعد التجريم والعقاب على هذه الجريمة.

رسالة ماجستير بعنوان: جريمة الارهاب الالكتروني، غلاف كريمة وجرلال زوهرة، جامعة عبدالرحمن ميرة: بجاية/ الجزائر، 2018.

هدفت هذه الدراسة الى تحديد مفهوم جريمة الارهاب الالكتروني وبيان دوافع ارتكابها وكذلك ابرز وسائل الارهاب الالكتروني التي يستعين بها الارهابيين والتي منها: البريد الالكتروني، وانشاء حسابات ومواقع خاصة بالتنظيمات الارهابية، واختراق المواقع الالكترونية وتدميرها، والتجسس الالكتروني، وهدفت ايضاً الى تحديد آليات التعامل مع هذه الجريمة موضوعاً واجراءاً في الجزائر.

رسالة ماجستير بعنوان: دور الضبط الاداري في مجال الجرائم الالكترونية المخلة بالأمن العام "دراسة تحليلية"، مصطفى جمال حنفي زينو، جامعة الازهر: غزة/فلسطين، 2017.

جاءت هذه الدراسة للبحث في سبل المواجهة المتاحة للوقوف امام الجرائم الالكترونية المخلة بالأمن العام وذلك لخطورتها ولانتشارها الواسع في وقتنا الحالي، ومن اهم هذه السبل الضبط الاداري، فتسعى هذه الدراسة لبيان آلية مواجهة هذه الجريمة التي تهدد الامن العام من خلال الاحكام والقواعد التي تحكم نظرية الضبط الاداري، وبيان مدى ملائمة هذه الاحكام التقليدية لمنع ارتكاب الجرائم الامنية المستحدثة، كما

هدفت لدراسة امكانية تحديث نظرية الضبط الاداري وتجديد وسائلها حتى تتلاءم مع طبيعة هذه الجرائم المستحدثة وذلك للحد من اضرارها التي تمس بأمن المجتمع بأكمله.

رسالة ماجستير بعنوان: جريمة الارهاب عبر الوسائل الالكترونية "دراسة مقارنة بين التشريعين الاردني والعراقي"، مصطفى سعد حمد مخلف، جامعة الشرق الاوسط: عمان/ المملكة الاردنية الهاشمية، 2017.

هدفت هذه الدراسة الى التعرف على الجرائم الالكترونية وبالأخص جرائم الارهاب الالكتروني، وموقف كل من المشرع الاردني والعراقي من هذه الجرائم، والاسباب وراء ارتكاب جرائم الارهاب الالكتروني والى ماذا يهدف الارهابيون، وتطرقت هذه الدراسة الى تبيان الاجراءات الجنائية لجريمة الارهاب الالكتروني والعقوبات المقررة لها في كل من التشريعين.

رسالة ماجستير بعنوان: الارهاب الالكتروني وتأثيره على امن الدولة، توفيق شريخي، جامعة مُحمَّد بوضياف: المسيلة/الجزائر 2017.

احاطت هذه الدراسة بجميع الجوانب الظاهرة والخفية للإرهاب الالكتروني وتأثيراته على امن الدولة، فتناولت اهم الاسباب التي تؤدي للإرهاب الالكتروني ووضحت طبيعة الاخطار التي تنجم عنه، كما تطرقت الى ابعاد ومستويات الامن (الوطني، والاقليمي، والدولي، والفردي)، وبحثت بالعلاقة بين الارهاب الالكتروني وامن الدولة، وجاء في هذه الدراسة اهم مظاهر الخطر في الارهاب الالكتروني والتي تتمثل في اختراق المواقع الالكترونية وخلق الفيروسات ونشرها، كذلك الحروب الاعلامية، والتجسس الالكتروني، والقصف الالكتروني وتدمير انظمة المعلومات. كما عرضت هذه الدراسة الجهود الوطنية في مكافحة الارهاب والاستراتيجيات الدولية لمكافحتها.

تتميز هذه الدراسة عن الدراسات السابقة في انها تناولت الاعتداءات الالكترونية من زاوية شمولية تربط بين البعد المفاهيمي والبعد التطبيقي، فقد تضمنت تعريفاً لكل من الاعتداءات الالكترونية والأمن الداخلي

وكذلك الأمن المعلوماتي ومن ثم تطرقت الى أهم صـــور الاعتداءات الالكترونية التي تقع على الأمن الداخلي للدولة.

كما تختلف هذه الدراسة في تركيزها على دور أجهزة العدالة في مكافحة الاعتداءات الالكترونية، من خلال تحليل الأدوار القانونية والتنظيمية لكل من جهاز الشرطة الفلسطينية (وحدة الجرائم الالكترونية)، والجهاز الوقائي الفلسـطيني. بالإضـافة الى تسـليطها الضـوء على الإجراءات الحديثة والمسـتحدثة في مكافحة الاعتداءات الالكترونية مع بيان مدى غياب او قصـور تنظيمها في التشـريع الفلسـطيني بالمقارنة مع التشريعات العربية الأخرى.

الفصل الأول

ماهية الاعتداءات الالكترونية على الامن الداخلي للدولة

شـهدت العقود الأخيرة تطوراً غير مسبوق في تكنولوجيا المعلومات والاتصـالات، ما أدى إلى بروز فضـاء إلكتروني جديد أصـــبح جزءاً لا يتجزأ من الحياة اليومية للأفراد والدول على حد ســـواء. ومع هذا التطور التقني، ظهرت تهديدات متعددة للأمن القومي، لا ســـيما تلك التي تتســـلل عبر الأدوات الرقمية، محدثة تحولات في طبيعة الاعتداءات التقليدية، وناشـــئة عن فاعلين قد يكونون مجهولي الهوية أو خارج الحدود الجغرافية للدولة. ومن أبرز التحديات التي باتت تواجهها الدول اليوم ما يُعرف بـ "الاعتداءات الإلكترونية"، وهي أعمال موجهة ضـد المصـالح الحيوية للدولة باسـتخدام الوسـائل التقنية، وتطال بنيتها السـياسـية، والأمنية، والاجتماعية، والاقتصادية (باطلي، 2015).

تُعد الاعتداءات الإلكترونية الواقعة على أمن الدولة الداخلي أحد أبرز التحديات القانونية والإجرائية التي تواجه الدولة المعاصـرة، في ظل تصـاعد وتيرة الجرائم المرتكبة عبر الفضـاء الرقمي. فقد باتت الهجمات المعلوماتية تمثل وسـيلة فعالة للمسـاس باسـتقرار الدولة وأمنها، من خلال اسـتهداف أنظمتها السـياسـية والاقتصـادية والاجتماعية، واسـتغلال الثغرات في التشـريعات والسـياسـات الأمنية، خاصـة في الدول ذات الأنظمة القانونية غير المتكاملة في المجال الرقمي، كما هو الحال في فلسطين.

إن مظاهر الاعتداءات الإلكترونية الواقعة على الأمن الداخلي تتنوع، فمنها ما يأخذ شكل التحريض العلني على العنف أو الفتنة الطائفية، ومنها ما يتجلى في حملات تشويه ضد رموز الدولة ومؤسساتها الرسمية، أو محاولات اختراق المواقع السـيادية، أو نشـر أخبار كاذبة تثير البلبلة العامة وتضـعف الثقة في الدولة ومؤسساتها. هذه الأفعال قد لا تجد توصيفًا قانونيًا دقيقًا ضمن النصوص التشريعية الحالية، رغم خطورتها الواضحة على الأمن الوطني (الحمامي و الحكيم، 2017).

كما أن التطور التقني أفرز أنماطًا جديدة من هذه الاعتداءات، مثل التزييف الإعلامي الرقمي، وحملات التأثير السياسي الممنهجة عبر الروبوتات الإلكترونية، واستخدام الذكاء الاصطناعي في إنشاء محتوى زائف يُستغل في سياقات سياسية أو أمنية. هذا التنوع في الأساليب يفرض على الباحثين والمهتمين بالقانون الجنائي والقانون العام فحص النصوص القانونية بعين نقدية، ودراسة مدى قابليتها للاستجابة لهذه التحديات (العقات، 2012).

بناءً عليه، فإن هذا الفصل يسعى بدايةً إلى توضيح ما المقصود بالاعتداء والجريمة الالكترونية، وكذلك توضيح المقصود بأمن الدولة الداخلي، ومن ثم الى بيان أبرز صور الاعتداءات الإلكترونية الواقعة على أمن الدولة الداخلي، مع تحليلها قانونيًا وفق ما هو منصوص عليه في القرار بقانون الفلسطيني بشأن الجرائم الإلكترونية، ومقارنتها بما هو معمول به في دول أخرى ذات تجربة تشريعية أكثر نضجًا في هذا المجال، بهدف بلورة تصور شامل لطبيعة التهديدات وكيفية مواجهتها تشريعيًا ومؤسساتيًا.

المبحث الأول: المقصود بالاعتداءات الالكترونية والامن الداخلي للدولة

يرتبط مفهوم الاعتداءات الالكترونية ارتباطاً وثيقاً بالأمن الداخلي للدولة، اذ أن هذه الاعتداءات قد تستهدف البنية التحتية المعلوماتية للدولة، او الرموز الوطنية والمؤسسات السيادية بما يؤدي الى زعزعة الاستقرار والامن العام وتقويض سيادة القانون. ومن هنا، فإن مواجهة هذه الظاهرة تستلزم اطاراً قانونياً متكاملاً يحدد أركانها وصورها والعقوبات المقررة لها.

وبناءً على ذلك، يصبح من الضروري اولاً توضيح المقصود بالاعتداء الالكتروني والامن الداخلي للدولة حتى يتسنى لنا تحليل هذه الاعتداءات تحليلاً قانونياً واستعراض اثارها على المجتمع والامن الداخلي الدولة.

المطلب الأول: الطبيعة القانونية للاعتداء الالكتروني

اعتداء: مصدر اعتدى والعادي هو الظالم. يقال: لا أشمت الله بك عاديك، أي عدوّك الظّالم لك، والاعتداء والتعدّي والعدوان: الظّلم (الهروي، 2001). ويأتي الاعتداء بمعنى العداوة، والعداوة: هي ما يتمكن في القلب من قصد الإضرار والانتقام (الجرجاني، 1983).

وورد الفعل (اعتدى) ومصـــدره (الاعتداء) في القرآن الكريم، ويراد به مجاوزة الحد، ومنه قوله تعالى: ﴿ وَمَن يَعْصِ ٱللَّهَ وَرَسُولَهُۥ وَيَتَعَدَّ حُدُودَهُۥ ﴾ [النساء: 14].

وفي اصـــطلاح الفقهاء يقصـــد به تجاوز الحد والقدر والحق الذي ينبغي الاقتصـــار عليه (وزارة الأوقاف والشؤون الإسلامية–الكويت، 1984).

أما الإلكترون فهو لفظ أعجمي[1] أقرّه مجمع اللغة العربية في مصر، وضمته المعاجم العربية الحديثة إليها، وقد جاء في المعجم الوسيط[2]: الإلكترون: "دقيقة ذات شحنة كهربائية سالبة، شحنتها هي الجزء الذي لا يتجزأ من الكهربائية".

والإلكتروني هو منسوب الى إلكترون، والالكترونيات فرع من علم الفيزياء والهندسة يتناول التحكم في انسياب الشحنات الكهربائية في وسائل معينة، لتحقيق أغراض مفيدة، وتستخدم المكوّنات الإلكترونية في مدى واسع من المنتجات، مثل أجهزة الراديو والتلفاز والحواســـيب (الموســـوعة العربية العالمية، د.ت). والمراد بكلمة إلكتروني في الأنظمة الحديثة هو الحواسيب.

وتعرّف الاعتداءات الالكترونية: هي كل الاعتداءات التي تهدف إلى إلحاق الضـــرر بأنظمة المعلومات فتؤثر بذلك على ســلامة المعلومات، ومصــدر توافر المعلومات وســريتها في هذه الأنظمة، حيث ان هذه

[1] أصل كلمة (إلكترون) يوناني، وهي تعني العنبر أو الكهرمان، وسبب ذلك أن الاغريق لاحظوا أن الكهرمان يجذب الأجسام الخفيفة عندما يدلك، ويبدو أن الإيرلندي ج. ستوني هو أول من استعملها عام1819. انظر: الموسوعة العربية الصادرة عن الجمهورية السورية (324/3 و330).

[2] مادة (الإلكترون)(24).

الاعتداءات تختلف درجة خطورتها باختلاف الدافع من الاعتداء، فمنها ما يكون بدافع سياسي، اقتصادي أو بدافع تجاري أو فردي ومنها من يقوم بالاعتداء من أجل الفضـــول والافتخار وغيرها من الاعتداءات (حديد و مسوس، 2016).

وهناك من عرّفها على انها تلك الاعتداءات التي قد تحدث للمعلومات داخل النطاق الالكتروني، مثل تلك المعلومات المخزنة في الحاسب الشخصي مروراً بالشبكة حتى جهاز الخادم، وتتضمن أساليب مختلفة كانتحال الشخصية، والاستخدام غير المرخص له، وعرقلة الخدمة، والتصنت والبرامج الخبيثة (المبارك، د.ت.).

ولفهم أوسع لمصطلح الاعتداء الالكتروني، ينبغي لنا تمييزه عن الجريمة الالكترونية:

الجريمة لُغةً هي اسم، مصدرها (جَرَمَ)، والجمع (جرائمُ)، جرم أي قطع الشيء، وأجرم عليه بمعنى أذنب واعتدى والجرم هو الخطأ (قاموس المعاني، د.ت.)، وهي بصورة عامة كلُّ أمر إيجابي أو سلبي يعاقب عليه القانون، سواء أكان مخالفة أم جنحة أم جناية.

يطلق مفهوم الجريمة في الإســـلام على ارتكاب كل ما هو مخالف للحق والعدل والطريق المســـتقيم، فقد قال تعالى في كتابه الكريم: ﴿ إِنَّ ٱلَّذِينَ أَجۡرَمُواْ كَانُواْ مِنَ ٱلَّذِينَ ءَامَنُواْ يَضۡحَكُونَ ﴾ [المطففين: 29]، وكذلك قوله تعالى: ﴿ كُلُواْ وَتَمَتَّعُواْ قَلِيلًا إِنَّكُم مُّجۡرِمُونَ ﴾[المرســـلات: 46]، فالجريمة هي فعل ما نهى الله عنه، وعصـــيان ما أمر الله به، ولذلك فقد قرر الله عز وجل عقابا لكل من يخالف أوامره ونواهيه، وهو إما أن يكون عقابا دنيويا ينفذه ولي الأمر، وإما عقابا في الآخرة ينفذه الحاكم الديان، وهو خير الفاصـــلين (أبو زهرة، 1998).

لقد درجت التشـــريعات المختلفة على عدم وضـــع تعريف للجريمة تاركةً ذلك للفقه والذي بدوره اختلف في تعريف الجريمة تبعاً لاختلاف وجهات النظر الفكرية، فمنهم من اعتمد في تعريف الجريمة على

الباعث لتجريم الافعال، ومنهم من اعتمد في تعريفه للجريمة على الركن القانوني فيها باعتباره الركيزة الاساسية لوجودها.

فقد عرّف الفيلسوف الفرنسي والمفكر الاجتماعي روسو الجريمة بأنها: " كل فعل من شأنه ان يفصم عرى العقد الاجتماعي الذي ينظم حياة الجماعة والذي قبل به كل فرد فيها من حاكم ومحكوم" (نجم، 2000).

حيث ان هذا التعريف يوضح قيام الدولة على اساس العقد الاجتماعي دون الاشارة الى الركن القانوني للجريمة ومن الفقهاء الذين ركزوا على ابراز الركن القانوني في تعريفهم للجريمة، الفقيه الايطالي كرارا فقد عرّف الجريمة بأنها: "انتهاك حرمات قانون من قوانين الدولة بفعل خارجي صادر عن رجل لا يبرره قيام بواجب، ولا ممارسة حقّ على ان يكون منصوصاً على معاقبته في القانون" (حومد، 1975).

وعرفها الفقيهان الفرنسيان ستيفاني وجورج لوفاسير بأنها: " فعل او امتناع عن فعل مسند الى صاحبه، ينص عليه القانون ويعاقب من اجله بعقوبة جزائية" (السراج، قانون العقوبات السوري – القسم العام، 1995).

فكما ذكرنا سابقا ان التشريعات لم تعرف الجريمة، فلم يرد في قانون العقوبات الاردني رقم 16 لسنة 1960 الساري في الضفة الغربية تعريفا لها، بل اكتفى ببيان الافعال التي تشكل جريمة سواء الايجابية او السلبية وبيان اركانها والعقوبة المقررة لكل منها.

وترى الباحثة من خلال التعريفات السابقة بأنه يمكن تعريف الجريمة على انها: كل فعل او امتناع عن فعل يخالف احكام القانون والذي بدوره يفرض على مرتكبه جزاء.

اما فيما يتعلق بالجريمة الالكترونية، لم يقم المشرع الفلسطيني بوضع تعريف للجريمة الالكترونية وانما اقتصر على سرد الجرائم او الافعال التي ينطبق عليها قانون الجرائم الالكترونية الفلسطيني، تاركا ذلك للفقه.

ومع هذا، تعددت تعاريف الفقهاء للجريمة الالكترونية وذلك بتعدد المعايير والاســس التي يعتمدونها، حيث انقسمت الى أربعة اتجاهات تقوم على أسس مختلفة وهي:

اولاً: على أساس وسيلة ارتكاب الجريمة

فهي تعريفات تعتمد على وســيلة ارتكاب الجريمة، والذي يعتبر اصـــحابها ان جريمة الحاســب تتحقق باســتخدام الحاســب كوســيلة لارتكاب الجريمة، حيث يعرفها فورســتر انها(هي الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيســياً)(Forester, 1989) ، ويرى الفقيه الألماني تاديمان أن الجرائم المعلوماتية هي "كل اشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي" (Tiedemann, 1989).

اي يمكننا القول بأن الجريمة الالكترونية حسب هذا المعيار عبارة عن فعل اجرامي يتم استخدام الحاسب في ارتكابه كأداة رئيسة.

ثانياً: على أساس موضوع الجريمة

يرى واضعو هذا التعريف أن الجريمة المرتكبة عبر الانترنت ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع عليه أو في نطاقه (الملط، 2006)، ومن أشـــهر فقهاء هذا الاتجاه الفقيه "Rosenblatt" الذي عرف جريمة الإنترنت بأنها: "نشاط غير مشروع موجه لنسخ، أو تغيير أو حذف، أو للوصول إلى المعلومات المخزّنة داخل الحاسب، أو التي تحول عن طريقه" (الرشيد، 2004).

ومن التعريفات التي تستند الى موضــوع الجريمة او احياناً الى انماط الســلوك محل التجريم تعرفها بأنها "كل ســلوك غير مشــروع او غير مســموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات" (قشقوش، 1992).

كما عرفها خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصـادية بأنها " كل سـلوك غير مشـروع ومناف للأخلاق او غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها".

فنستنتج هنا ان أصـحاب هذا الاتجاه ذهبوا لتصـنيف الجريمة الالكترونية بأنها افعال غير مشروعة، يكون الهدف من ورائها الوصول الى معلومات معينة او حذف هذه المعلومات او تغييرها داخل الحاسب الآلي.

ثالثاً: على أساس توافر المعرفة بتقنية المعلومات

أي يستند انصار هذا الاتجاه في تعريفهم للجريمة الالكترونية على السمات الشخصية لمرتكبها، بمعنى ان يكون ملماً بتقنية المعلومات. ومن هذه التعريفات: " كل سـلوك غير مشـروع يكون العلم بتكنولوجيا الحاسـبات الآلية بقدرٍ لازم لارتكابها من ناحية، وملاحقته وتحقيقه من ناحية أخرى" (عبد الحكيم م.، 2015). وكذلك عرّفها الفقيه "David Thomson" بأنها " أيّة جريمة يكون متطلباً لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسـب" (Thomson, 1991)، او "هي ذلك النوع من الجرائم الذي يتطلب الماماً خاصـاً بتقنيات الحاسب الآلي ونظم المعلوماتية لارتكابها أو التحقيق فيها ومقاضـاة فاعلها" (عياد، 2007)، وهذا تعريف ضـيّق للجريمة الالكترونية، فهو يضـيّق من دائرة الأشـخاص الذين يعتبرون مرتكبي لهذه الجريمة، حيث يمكن أن يتم ارتكاب بعضها دون ان يكون المرتكب على دراية عميقة بتقنيات الحاسب الالي والشبكة المعلوماتية.

رابعاً: اتجاه يأخذ بدمج عدة تعاريف

عمد أصـحاب هذا الاتجاه الى تعريف الجريمة الالكترونية تعريفاً شـاملاً عن طريق دمج اكثر من عنصـر او معيار فاعتبروها بأنها " الجريمة التي يسـتخدم فيها الحاسـب الآلي كوسـيلة أو أداة لارتكابها أو يمثل اغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيتها (الرشيد، 2004، الصفحات 108-109)، ومنهم من عرّفها بأنها: "كل نشـاط إيجابي أو سـلبي من شـأنه الاتصـال والتأثير في الكيان المعنوي للحاسـب الآلي بتعطيله، أو إضـعاف قدرته على أداء وظائفه بالتأثير على برامجه، أو المعلومات المخزنة به بالنسـخ، أو

التعديل بالحذف أو بالإضافة أو المناقلة في الخصائص الأساسية للبرامج أو المعلومات، أو الحذف الكلي، أو الجزئي، أو الوصول إلى البرامج أو المعلومات المخزنة به، أو الوصول إليها أثناء نقلها، أو إرسالها، أو الاتصال به، أو الإبقاء على الاتصال من غير وجه حق" (الهيتي، 2006)' فشمل هذا التعريف في وصفه للجريمة الالكترونية كل فعل إيجابي او سلبي، دون وجه حق، يتصل بواسطة حاسب الي كوسيلة للجريمة، بشبكة الانترنت وهي المجال المعنوي، حيث يتم تبادل البيانات كمحل للجريمة وذلك عن طريق نسخ أو حذف او لصق للبيانات للوصول الى معلومات مخزنة ذات قيمة.

ولعل أفضل تعريف وضع للجريمة الالكترونية الذي تم تبنيه من قبل مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين وهو " أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" (الأمم المتحدة، 10-17 نيسان 2000)، فهذا التعريف أحاط بجميع الاشكال الإجرامية للجريمة الالكترونية، سواء التي تقع بواسطة حاسب آلي، او تلك التي تقع على البيانات والبرامج داخل نظام معلوماتي، واية جريمة قد تقع داخل بيئة إلكترونية.

من خلال التعريفات السابقة يتضح لنا ما يلي في تعريف الجريمة الالكترونية:

1. قد يكون الجهاز هدفاً للجريمة ذاتها، اي هو محل الجريمة، وذلك كما في حالة الدخول غير المصرح به الى نظام ما، او زرع الفيروسات به لتدمير البيانات الموجودة.
2. او ان يكون اداة الجريمة، اي استخدام الحاسب الالي للقيام بالجريمة، كاستخدامه كوسيلة في عمليات التزوير، او للاستيلاء على الاموال بإجراء تحويلات غير مشروعة عبر الانترنت بهدف غسيل الاموال وغيرها من الجرائم.
3. الاعتداء واقع على مصلحة يحميها القانون.
4. توافر حد ادنى من المعرفة التقنية لدى الجاني.

وبناءً على ذلك، يمكن تعريف الجريمة الالكترونية على انها: نشـــاط يقوم به الشـــخص باســـتخدام التقنية الالكترونية (الحاسب الالي وشبكة الانترنت) كوسيلة لتنفيذ الفعل الذي يعاقب عليه بالقانون.

وبهذا تســتنتج الباحثة بأن الاعتداء هو عبارة عن ســلوك يقوم به الشــخص، ولم تشــمله التشــريعات، اما الجريمة تتطلب وجود نص تشريعي واضح وصريح، يجرّم الفعل المرتكب ويحدد له العقوبة المناسبة، فيبرز الفارق بين "الاعتداء" و"الجريمة"، إن كثيرًا من الأفعال لا تخضـــع لعقوبات قانونية صـــريحة، لعدم وجود نصوص تُجرّمها بشكل مباشر.

المطلب الثاني: التعريف بالأمن الداخلي للدولة والأمن المعلوماتي

الامن لغةً: الهمزة والميم والنون أصــلان متقاربان: احدهما الامانة التي هي ضــد الخيانة، ومعناها ســكون القلب، والآخر التصديق (ابو الحسين، د.ت.)، والأمن يعني الاستقرار والاطمئنان، يُقال: أمن منه أي سلم منه، وأمن على ماله عند فلان أي جعله في ضــمانه، والأمان والأمانة بمعنى واحد، فالأمن ضــد الخوف، والأمانة ضد الخيانة، والمأمن الموضع الأمن (ابن منظور، 2000).

وردت كلمة الأمن وما يشتق منها في مواضع عديدة من القرآن الكريم، والتي تعني السلامة، وانتفاء الخوف على حياة الانسان، او على ما تقوم به حياته من مصالح وأهداف وكذلك امن المجتمع ككل.

يقول الله تعالى:

﴿ وَإِذْ قَالَ إِبْرَٰهِـۧمُ رَبِّ ٱجْعَلْ هَٰذَا بَلَدًا ﴾ [البقرة: 126].

﴿ وَلَيُبَدِّلَنَّهُم مِّنۢ بَعْدِ خَوْفِهِمْ أَمْنًا ۚ ﴾[النور: 55].

وفي السنة النبوية، ما يؤكد اهمية أمن الانسان في الجماعة التي يعيش فيها، يقول (ﷺ):

(مَنْ أَصْـــبَحَ مِنْكُمْ آمِنًا فِي سِـــرْبِهِ، مُعَافًى فِي جَسَـــدِهِ، عِنْدَهُ قُوتُ يَوْمِهِ، فَكَأَنَّمَا حِيزَتْ لَهُ الدُّنْيَا) رواه البخاري في "الأدب المفرد" (رقم/300) والترمذي في "السنن" (2346).

ويعني في سِربه: في نفسه، وقيل: السرب: الجماعة، فالمعنى: في أهله وعياله. وقيل بفتح السين أي: في مسلكه وطريقه، وقيل بفتحتين أي: في بيته.

فالأمن يعكس السلام او الطمأنينة والسكينة في المكان والزمان الذي يعيش فيه الانسان سواء على نفسه او عرضه او ماله او افكاره وعقيدته.

اما الفقه، فقد تباينت تعريفات الفقهاء لمصطلح أمن الدولة الداخلي، فمنهم من عرفه بأنه " الكيان المادي والمعنوي للدولة في أعين المحكومين بها، فالكيان المادي هو وجودها الواقعي وإحساس المواطنين بسطوتها، وبأنها قابضة على زمام الأمور والكيان المعنوي هو احترام المواطنين وولائهم نحوها (بهنام، 1990).

وعرفه البعض ايضاً بأنه الاجراءات الخاصة بتأمين الفرد داخل الدولة ضد الاخطار الماسة بالنفس والمال ووضع التشريعات التي تحقق حمايته والحفاظ على مقدساته من خلال اجهزة الامن الداخلي بمنع وقوع الجرائم وانشاء الأجهزة القضائية لتوقيع العقاب على الخارجين عن القانون (اللبيدي، 2010).

حاولت محكمة القضاء الإداري المصرية في حكمها الصادر في الدعوى رقم 21855 لسنة 65 القضائية اثناء نظر دعوى قطع الاتصالات خلال ثورة يناير 2011 تعريف الأمن القومي بأنه " ومع تطور قدرة الدولة اتسع مفهوم الأمن القومي إلى القدرة الشاملة للدولة والمؤثرة على حماية قيمها ومصالحها من التهديدات الخارجية والداخلية، ولذلك كان للأمن القومي ابعاداً سياسية، واقتصادية، واجتماعية، وعسكرية، وأيدلوجية، وجغرافية، ولكل بُعد خصائصه التي تثبت ترابط تلك الأبعاد وتكاملها، فالبعد السياسي للأمن القومي ذو شقين داخلي وخارجي، يتعلق البعد الداخلي بتماسك الجبهة الداخلية وبالسلام الاجتماعي وبالمواطنة وتراجع القبلية والطائفية بما يحقق دعم الوحدة الوطنية..." (حكم محكمة القضاء الإداري المصري الصادر في الدعوى رقم 21855 لسنة 65 قضائية، 2011).

فيما يتعلق بالتشريعات، لم يرد في قانون العقوبات الاردني رقم 16 لسنة 1960 الساري في الضفة الغربية تعريفاً لمصطلح امن الدولة الداخلي، انما تناول في الباب الاول الخاص بالجرائم التي تقع على امن الدولة تعداد لهذه الجرائم الماسة بأمن الدولة، حيث قسمها الى فصلين، الفصل الاول يتعلق بالجرائم التي تقع على امن الدولة الخارجي، والفصل الثاني يتعلق بالجرائم الواقعة على امن الدولة الداخلي والتي سنتناولها لاحقاً.

مما سبق يمكن القول بأنه لا يوجد تعريفاً جامعاً مانعاً لمصطلح أمن الدولة الداخلي، ويرجع السبب في ذلك ان الامن يعتبر حقيقة متغيرة تتأثر بعوامل عديدة سواء داخلية ام خارجية.

التمييز بين امن الدولة الداخلي والامن المعلوماتي

فرض التطور الالكتروني الهائل والمتسارع على المجتمعات الاعتماد على تقنيات تكنولوجية في شتى مجالات الحياة والعمل، حيث أصبحت التكنولوجيا جزءً لا يتجزأ من حياتنا اليومية، فهي تشغل حيزاً كبيراً سواء في تواصلنا ومعاملاتنا اليومية أو المهنية، من خلال مجتمع افتراضي نشأ كنتيجة لهذا التطور وهو موازي للمجتمع الواقعي التقليدي، والذي مكّن مختلف الفئات الاجتماعية من دخول هذا المجتمع بكل سهولة، وممارسة سلوكيات وانشطة عديدة قد تكون من شأنها ان تمس ليس فقط الحياة الخاصة للأفراد، بل تمتد لتشمل جانب آخر وهو امن الدولة، الامن العام داخل المجتمع التقليدي سواء الداخلي ام الخارجي، او حتى الافتراضي، فهذا الاخير مليء بالبيانات التي بحاجة لحماية، وهذا ما نقصده بالأمن المعلوماتي.

يمكن تعريف امن المعلومات من ثلاث زوايا، وهي (كردي، 2011):

- من زاوية اكاديمية: انه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من انشطة الاعتداء عليها.
- من زاوية تقنية: هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية.

- من زاوية قانونية: فإن امن المعلومات هو تدابير حماية ســـرية وســـلامة محتوى وتوفر المعلومات، ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة.

وورد في القرار الصادر من مجلس الوزراء رقم 16 لسنة 2015 (المتعلق بالنظام الداخلي لعمل الفريق الفلسطيني للاستجابة لطوارئ الحاسوب) تعريفاً للأمن السيبراني في المادة (1) منه وهو " مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية وإدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتكنولوجيا التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستعملين، وتشمل أجهزة الحوسبة الموصولة بالشبكة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة و/أو المحفوظة في البيئة السيبرانية".

فيستنتج ان الامن المعلوماتي او الالكتروني هو عبارة عن مجموعة من الاجراءات او التدابير الوقائية التي تستخدم للمحافظة على المعلومات او البيانات وخصوصيتها، حيث جاء في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات تعريف البيانات والمعلومات الالكترونية في المادة 1 منه: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الارقام أو الحروف أو الرموز أو الاشارات، وغيرها.

وكذلك عرّف تكنولوجيا المعلومات بأنها: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة.

فبالتالي نستنتج ان امن الدولة بشكل عام قد يكون عرضة للخطر او الاعتداء اما بطريقة تقليدية داخل المجتمع التقليدي كالاضطرابات واعمال الشغب او اثارة عصيان المسلح وغيره، واما بطريقة الكترونية كالقيام

بأي نشاط الكتروني يهدد امن الدولة مثل التحريض على الفتنة او نشر الشائعات التي من شأنها أن تهدد الأمن الوطني عن طريق شبكات التواصل الاجتماعي، او الارهاب الالكتروني وغيرها من الاعتداءات.

المبحث الثاني: صور الاعتداءات الالكترونية على أمن الدولة الداخلي

تُعد الصور التقليدية للاعتداءات على أمن الدولة الداخلي مدخلاً أساسياً لفهم الأشكال المستقرة من التهديدات السيبرانية التي واجهتها الدول منذ المراحل الأولى للتحول الرقمي. هذه الصور لا تزال تشكل النواة الرئيسية للاعتداءات التي تمارس ضد استقرار الدولة ونظامها السياسي والاجتماعي، رغم تطور الوسائل والأساليب التقنية المستخدمة. ومن المهم إدراك أن الاعتداءات التقليدية قد اتخذت منحى جديداً في الفضاء الإلكتروني، مع الحفاظ على غاياتها القديمة: زعزعة الثقة بالمؤسسات، الإخلال بالنظام العام، وبث الشائعات التي تستهدف السلم الأهلي (العريشي و الشلهوب، 2016).

تشمل هذه الصور العديد من الأفعال التي تُمارس بوسائل تقنية حديثة، مثل التحريض على الكراهية، التشهير برموز الدولة، ونشر الشائعات التي تؤثر على الرأي العام، وهي أفعال كانت تُرتكب في الماضي عبر الوسائل التقليدية كالصحف والمنشورات، إلا أنها اليوم تتخذ شكل منشورات رقمية، وفيديوهات، وبث مباشر، وحملات منظمة على شبكات التواصل. وهنا تكمن خطورتها، إذ أن انتشارها واسع، وصعوبة ملاحقتها القانونية كبيرة، وفعاليتها في التأثير أكبر من الوسائل السابقة (محمود و دراج، 2022).

كما يكمن الخطر الحقيقي في أن هذه الاعتداءات لا تقتصر على الأثر اللحظي، بل تعمل على زعزعة الثقة بالمؤسسات، وتفكيك النسيج الاجتماعي، والتأثير على استقرار الدولة من الداخل من خلال أدوات تبدو في ظاهرها مشروعة كحرية التعبير، لكنها تُستغل بطريقة موجهة تخدم أجندات داخلية أو خارجية.

في الحالة الفلسطينية، يزداد الأمر تعقيدًا نظرًا لخصوصية الوضع السياسي وغياب السيادة الكاملة على الفضاء الرقمي، بالإضافة إلى نقص التشريعات التي تعالج بشكل مباشر هذا النوع من الأفعال. ومع أن القرار بقانون بشأن الجرائم الإلكترونية لسنة 2018 وضع أساسًا قانونيًا عامًا، إلا أنه لم يفصل الاعتداءات

على النظام السياسي بالصيغة التي تتناسب مع طبيعتها الحديثة، ما يترك فجوة قانونية خطيرة في حماية الأمن الداخلي للدولة.

من الناحية المقارنة، تظهر بعض النماذج التشريعية المتقدمة في هذا السياق، مثل النموذج الأردني، والمشرع الاماراتي الذي نص صراحة على الاعتداءات الواقعة على أمن الدولة في قوانين الجرائم الإلكترونية، أو التشريع المصري الذي أولى اهتمامًا خاصًا بحماية البنية التحتية الرقمية للدولة، وربط الأمن السيبراني بالأمن القومي في قوانين محددة (محمود و دراج، 2022).

من هذا المنطلق، يتناول هذا المبحث تصنيف وتحليل أبرز صور هذا النوع من الاعتداءات الإلكترونية وتحليل موقف القانون الفلسطيني منها، ومدى توافقه أو تباينه مع النماذج القانونية الأخرى، في محاولة لصياغة تصور متكامل حول واقع الحماية القانونية لهذا النوع من الاعتداءات.

المطلب الأول: التحريض على الفتنة الداخلية عبر الوسائط الإلكترونية

في ظل التحولات الرقمية المتسارعة، أصبح التحريض الإلكتروني يمثل أحد أبرز التحديات التي تواجه الدول في سعيها للحفاظ على النظام العام والاستقرار السياسي. يُفهم التحريض الإلكتروني على أنه استخدام الوسائل الرقمية، مثل وسائل التواصل الاجتماعي، المنتديات الإلكترونية، والمدونات، لنشر محتوى يهدف إلى إثارة الفتنة، التحريض على العنف، أو الدعوة إلى تقويض النظام السياسي القائم. يتميز هذا النوع من التحريض بقدرته على الوصول إلى جمهور واسع بسرعة فائقة، مما يزيد من تأثيره وخطورته على السلم الأهلي (المصري، 2011).

التحريض الإلكتروني لا يقتصر على الدعوة المباشرة للعنف، بل يشمل أيضًا نشر الشائعات، المعلومات المضللة، والترويج لأفكار تهدف إلى زعزعة الثقة في المؤسسات الحكومية. هذا النوع من التحريض يمكن أن يؤدي إلى تفكك النسيج الاجتماعي، تصاعد التوترات الطائفية أو العرقية، وإضعاف شرعية الدولة في نظر مواطنيها. في السياق الفلسطيني، تتفاقم هذه التحديات بسبب الوضع السياسي المعقد، والانقسام

الداخلي، والضـــغوط الخارجية، مما يجعل التحريض الإلكتروني أداة فعالة في يد الجهات الســـاعية إلى زعزعة الاستقرار.

هذا ما يدعو الباحثة في البحث عن مدى المســـؤولية القانونية المترتبة على مثل هذا النوع من الاعتداء، حيث نجد ان القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018 لم ينص صراحةً على تجريم فعل التحريض، وانما تناول بعض جوانبه، حيث يجرم القانون الأفعال التي تمس النظام العام أو الســـلم الأهلي عبر الوسـائل الإلكترونية، لكنه لا يقدم تعريفًا دقيقًا للتحريض الإلكتروني، ولا يحدد المعايير التي يمكن من خلالها تمييزه عن حرية التعبير المشـروعة. الامر الذي يفتح المجال أمام تفسـيرات متعددة قد تعيق تطبيق القانون بشكل عادل وفعال.

جاء في المادة (24) القرار بقانون بشـأن الجرائم الالكترونية ما يجرّم هذا النوع من الافعال التي تؤثر على السلم والامن المجتمعي حيث نصت على:

" كل من أنشـأ موقعاً أو تطبيقاً أو حسـاباً إلكترونياً أو نشـر معلومات على الشـبكة الإلكترونية أو إحدى وسـائل تكنولوجيا المعلومات، بقصـد عرض أي كلمات مكتوبة أو سـلوكيات من شـأنها أن تؤدي إلى إثارة الكراهية العنصـرية أو الدينية أو التمييز العنصـري بحق فئة معينة بسـبب انتمائها العرقي أو المذهبي أو اللون أو الشكل أو بسبب الإعاقة، يعاقب بالحبس مدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

ان الوسيلة الأساسية المستخدمة في هذه الجريمة هي الوسائط الإلكترونية، والتي تشمل: كل وسيلة رقمية أو تقنية تُستخدم لنقل أو نشر الأفكار والمعلومات، مثل الإنترنت، منصات التواصل الاجتماعي، تطبيقات الهاتف المحمول، البريد الإلكتروني، المدونات، ومواقع الفيديو وغيرها (السنوسي، 2018).

ويتحقق الركن المادي من خلال قيام الجاني بنشـر، بث، إرسـال، أو إعادة نشـر محتوى إلكتروني يتضـمن عبارات أو إشارات أو صورًا أو تسجيلات تحمل طابعًا تحريضيًا يهدف إلى إثارة النعرات الطائفية أو القبلية

أو المناطقية، أو الدعوة إلى التمييز أو الكراهية أو العنف بين مكونات المجتمع. ويكفي لقيام هذا الركن أن يكون الفعل من شـأنه أن يؤدي – ولو نظريًا – إلى تهديد السـلم الأهلي أو الإضـرار بالنظام العام، دون حاجة إلى تحقق النتيجة فعليًا. فالجريمة هنا تصـنف ضـمن "جرائم الخطر" وليس من ضـمن "جرائم الضـرر"، أي أن القانون يعاقب عليها لكونها تُحدث احتمالًا بوقوع ضـرر جسـيم، حتى وإن لم يقع فعليًا. حيث تُعرف جريمة الضرر بأنها الجريمة التي يفترض فيها وجود سلوك جرمي ترتبت عليه آثار متمثلة في الاعتداء الفعلي الحال على الحق المحمي قانوناً، أما جريمة الخطر فتعرف على انها تلك الجريمة التي تمثل عدوان محتمل على الحق أي وجود تهديد واقع عليه بالخطر (السراج، شرح قانون العقوبات – القسم العام، 1999).

وعليه، لا يشترط أن تنشأ فتنة فعلية أو اضطرابات داخلية أو أن تُزهق الأرواح أو تُسفك الدماء، بل يكفي أن يكون المحتوى المنشـور قادرًا بطبيعته، أو في ظل ظروف المجتمع، على التأثير السـلبي في التماسـك الاجتماعي، وبث بذور الشقاق والانقسام. ويُراعى في هذا السياق عنصر التكرار ومدى انتشار المحتوى، ومدى تأثيره في فئة مستهدفة أو في لحظة زمنية حساسة سياسيًا أو اجتماعيًا (الصيفي، 1967).

يُعد الركن المعنوي من أهم أركان جريمة التحريض على الفتنة الداخلية، إذ إنه يكشـف عن الباعث الذهني والنفسي للجاني في ارتكاب الفعل المحظور. وهذه الجريمة من الجرائم العمدية التي تقوم على توافر القصد الجنائي بصـورته العامة والخاصـة. ويتجسـد القصـد الجنائي العام في علم الجاني بطبيعة المحتوى الذي ينشـره أو يروجه، أي علمه بأن المادة التي يبثها تحتوي على دعوة للتحريض على الفتنة، مع إدراكه لما قد ينجم عنها من زعزعة الاسـتقرار أو الإضـرار بالسـلام المجتمعي. وهذا يتطلب أن يكون الجاني مدركاً لخطورة محتواه ومتعمداً إيصـاله إلى الجمهور، سـواء بشـكل مباشـر أو من خلال التفاعل مع محتوى تحريضي سبق نشره (مهدي، 2011).

أما القصـــد الجنائي الخاص، فيتحقق حين يثبت أن الجاني تعمّد إثارة الكراهية أو النزاع أو التمييز بين مكونات المجتمع، وكان يهدف إلى تحقيق غرض معين، مثل زعزعة النظام العام، أو إشـــعال الأوضـــاع الداخلية، أو التأثير على الرأي العام لأسباب سياسية أو طائفية أو أيديولوجية. ويُظهر هذا القصد الخاص نية الجاني في اسـتخدام الوسـائط الإلكترونية كأداة لبث الفتنة، مسـتغلًا سـرعتها في الانتشـار وسـهولة الوصـول إلى جماهير واسـعة. وفي بعض الحالات، يُسـتدل على القصـد الخاص من طبيعة المحتوى، والعبارات المستخدمة، وتكرار النشر، وتوقيت بث الرسائل، وعلاقته بسياقات اجتماعية أو سياسية حساسة. وفي ضوء ذلك، فإن المحاكم غالبًا ما تنظر في مجمل الظروف والملابسات المحيطة بالفعل، بما في ذلك السـوابق الجنائية للجاني، وانتماءاته السـياسـية أو الأيديولوجية، ومواقفه العلنية السـابقة، لتكوين تصـور واضـح حول نية التحريض ومدى تعمدها. كما تأخذ بالاعتبار مدى اسـتجابة الجمهور للمحتوى المحرض، وإن لم يكن ذلك شرطًا لقيام الجريمة، إلا أنه يعد مؤشراً مساعداً في تحليل البعد الذهني للجاني (الشواربي، التعليق الموضـــوعي على قانون العقوبات – الأحكام العامة لقانون العقوبات في ضـــوء الفقه والقضـــاء (الكتاب الأول)، 2003).

ووفقاً للمادة 24 من القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018 تنص على عقوبة اقصاها سنة لجريمة اثارة الكراهية، بمعنى ان للقاضي سلطة تقديرية في توقيع العقوبة والتي تتراوح بين الحد الادنى لعقوبة الحبس والحد المنصـــوص عليه، أي من اســبوع الى ســنة. وكذلك بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أي يمكن للقاضـــي ان يحكم فقط بالغرامة دون الحبس، وكذلك يمكن ان يحكم بكلتا العقوبتين.

وبالرجوع للمادة 64 من هذا القرار بقانون، والتي تنص على انه: " مع عدم الإخلال بأي عقوبة أشد، ينص عليها قانون العقوبات الســاري أو أي قانون آخر، يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات المنصوص عليها فيه".

وهذا ما يتيح للقاضـــي الرجوع الى نص المادة 150 من قانون العقوبات الأردني رقم 16 لســنة 1960: " كل كتابة وكل خطاب أو عمل يقصد منه أو ينتج عنه إثارة النعرات المذهبية أو العنصرية أو الحض على النزاع بين الطوائف ومختلف عناصر الأمة يعاقب عليه بالحبس مدة ستة أشهر إلى ثلاث سنوات وبغرامة لا تزيد على خمسين ديناراً".

بالمقارنة مع التشريع الأردني، نجد أن قانون الجرائم الإلكترونية الأردني يتضمن نصوصًا أكثر تحديدًا فيما يتعلق بالتحريض عبر الوسـائل الإلكترونية، حيث يجرم القانون الأردني الأفعال التي تهدف إلى إثارة الفتنة أو النعرات الطائفية أو العرقية، ويحدد العقوبات المناســبة لها، حيث نصـــت المادة 17 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023 على انه " يعاقب كل من قام قصداً باستخدام الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقع الكتروني أو منصـة تواصـل اجتماعي لنشـر ما من شـأنه إثارة الفتنة أو النعرات أو تستهدف السلم المجتمعي أو الحض على الكراهية أو الدعوة الى العنف أو تبريره أو ازدراء الأديان بالحبس من سنة الى ثلاث سنوات أو بغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (20000) عشرين ألف دينار أو بكلتا هاتين العقوبتين"[1]. حيث شدد العقوبة المترتبة على الفعل وذلك على خلاف ما جاء في التشـريع الفلسـطيني، وكما يميز بين حرية التعبير والتحريض الضـــار، مما يوفر إطارًا قانونيًا أكثر وضوحًا للتعامل مع هذه القضايا دون المساس بالحقوق الأساسية للمواطنين.

ويعتبر التشريع الإماراتي من اكثر التشريعات العربية التي تناولت صراحةً فعل التحريض الالكتروني، حيث جرّم التحريض على المساس بأمن الدولة أو النظام العام باستخدام الشبكة المعلوماتية، وذلك في المادة 23 من المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الالكترونية، فنصت على " يعاقب بالسـجن المؤقت والغرامة التي لا تزيد على (1000000) مليون درهم كل من أنشـأ أو أدار موقعاً إلكترونياً أو أشـرف عليه أو اسـتخدم معلومات على الشـبكة المعلوماتية أو وسـيلة تقنية المعلومات بقصـد

[1] حكم صادر من محكمة صلح عمان 11 حزيران 2024 بالحبس سنة اعمالاً بأحكام المادة 17 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023. https://www.alquds.co.uk/السجن-لمدة-عام-ضد-صحافية-أردنية-بسبب-نش/

التحريض على أفعال أو نشر أو بث معلومات أو أخبار أو رسوم كرتونية أو أي صور أخرى، من شأنها تعريض أمن الدولة ومصالحها العليا للخطر أو المساس بالنظام العام، أو الاعتداء على مأموري الضبط القضائي أو أي من المكلفين بتنفيذ أحكام القوانين"، وكذلك نص المادة 24 من ذات المرسوم التي عاقبت على من ينشئ او يدير موقعاً الكترونياً أو يشرف على أي موقع، أو ينشر ما يتضمن اثارة للفتنة أو الكراهية او العنصرية او الترويج أو التحبيذ لاي منها باستخدام شبكة المعلومات اذا كان من شأنها الاضرار بالسلم المجتمعي والنظام العام[1].

وترى الباحثة ان التحريض الإلكتروني يمثل تحديًا قانونيًا وأمنيًا كبيرًا، يتطلب من الدول تطوير تشريعاتها لتواكب التطورات التكنولوجية وتحديات العصر الرقمي. بالنسبة لفلسطين، هناك حاجة ملحة لتحديث الإطار القانوني الحالي، وصياغة تشريعات تنظم هذا الاعتداء، على شاكلة القانون الاماراتي، وتحديد مفاهيم واضحة للتحريض الإلكتروني، ووضع معايير دقيقة لتمييزه عن حرية التعبير، وتحديد العقوبات المناسبة له. كما يجب تعزيز قدرات الجهات المعنية على رصد ومكافحة هذا النوع من الجرائم، من خلال التدريب والتعاون مع الجهات الدولية المختصة.

المطلب الثاني: نشر معلومات كاذبة تؤثر على الرأي العام

يمكن أن يؤدي نشر الشائعات او الاخبار الكاذبة إلى إثارة الفتن والانقسامات داخل المجتمع، كما يمكن أن يستخدم كأداة للتحريض على العنف أو تقويض الاستقرار السياسي. في ظل هذه التحديات، يصبح من الضروري وجود تشريعات واضحة وصارمة لمكافحة هذه الظاهرة. ومع ما توفره المنصات الالكترونية من سرعة فائقة في نشر الاخبار والمعلومات، فإن ذلك يؤثر بشكل كبير على الرأي العام وزعزعة الثقة في

[1] المادة 24 من المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الالكترونية : " يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (200000) مائتي ألف درهم ولا تزيد على (1000000) مليون درهم كل من أنشأ أو ادار موقعاً إلكترونياً أو أشرف عليه أو نشر معلومات أو برامج أو أفكار تتضمن إثارة للفتنة أو الكراهية أو العنصرية أو الطائفية أو الترويج أو التحبيذ لأي منها باستخدام الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات و إذا كان من شأنها الإضرار بالوحدة الوطنية أو السلم الاجتماعي أو الإخلال بالنظام العام أو الآداب العامة أو تعريض مصالح الدولة للخطر."

المؤسسات الرسمية، خاصة في فلسطين، لما يخلّفه الوضع السياسي والانقسام الداخلي من تعقيدات ما يجعل المجتمع اكثر عرضة للتضليل.

تولّى الفقه القانوني الجنائي وضع التعريفات لجريمة بث الأخبار والإشاعات الكاذبة حيث عرفها أغلب الفقه بأنها رواية عن أمرٍ أو حدثٍ أو شخصٍ بأسلوب يروى أو يذاع، فهو نوع من الخبر غير المؤكد، ويريد قائله أن يلفت النظر إلى تأكيده وعلم الناس به (الشواربي، جرائم الصحافة والنشر وقانون حماية حق المؤلف والرقابة على المصنفات الفنية في ضوء القضاء والفقه، 1997).

وتعرّف الشائعة الالكترونية بأنها القضية أو الخبر أو الموضوع الذي يتم تداوله من خلال مواقع التواصل الاجتماعي عبر الانترنت أو الهواتف المحمولة، وتنتقي هذه الشائعة مادتها من مصادر متنوعة تختلف عن الشائعة التقليدية من حيث البناء والمحتوى، حيث يعبّر عنها بالنص المكتوب والصور والصوت والرسوم المتحركة كالفيديو (الحربي، 2012).

وهناك من عرّفها على أساس الغاية غير المشروعة التي تهدف لها الشائعة والذي يتمثل بالإضرار بالأمن الوطني فهي " خبر مدسوس كلياً او جزئياً وينتقل شفهياً أو عبر وسائل الإعلام دون أن يرافقه أي دليل أو برهان، ويقصد به تحطيم المعنويات (الخشت، 1996). فيمكن القول بأن الشائعات هي مجموعة من الأفكار التي يتم بثها لإحداث بلبلة في المجتمع، وزعزعة الامن والاستقرار، ويتم استغلال الوسائل التكنولوجية في الترويج لها نظراً لسرعة حدوث ذلك من خلالها.

اما محكمة صلح جزاء عمان فعرّفت الاخبار الكاذبة عبر الشبكة المعلوماتية " بأنه الخبر أو مجموعة من الأخبار الزائفة وغير الصحيحة التي تنتشر عبر الشبكة المعلوماتية ولا يكون لها مصدر موثوق، ويجري تداولها بين الناس بهدف التأثير على الأمن والسلم المجتمعي، وقد تكون ذات طابع عسكري أو سياسي أو اقتصادي أو اجتماعي"[1] (القرار الصادر عن محكمة صلح جزاء عمان، 2023).

[1] انظر : https://www.sarayanews.com/article/879705

فيما يتعلق بالقرار بقانون بشـأن الجرائم الالكترونية رقم 10 لسـنة 2018، نجد بأنه لم ينص صـراحةً على تجريم هذا الفعل، فلم يتناول جريمة الشـائعات الالكترونية التي تسـتهدف النيل من مؤسـسـات الدولة بشـكل مفصّـل، انما أدرجت بطريقة غير مباشـرة وذلك عندما اعطى المشـرع الصـلاحية لجهات التحري والضـبط المختصـة بحجب أي موقع يتضـمن ما من شـأنه تهديد الأمن القومي أو النظام العام أو الآداب العامة في نص المادة 59 حسـب التعديل الأخير القرار بقانون رقم 38 لسـنة 2021، وكذلك ما جاء في المادة 30 " كل من نشر قصـداً معلومات عن موقع الكتروني محجوب بموجب احكام المادة 39 من هذا القرار بقانون، باسـتخدام أنظمة أو موقع أو تطبيق إلكتروني، يعاقب بالحبس مدة لا تقل عن ثلاثة أشـهر، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

على عكس التشريع الأردني والذي تناول بشكل صريح جريمة نشر الشائعات او الاخبار الكاذبة وذلك في المادة 15 من قانون الجرائم الإلكترونية رقم 17 لسنة 2023 حيث نصت على انه: " أ. يعاقب كل من قام قصـداً بإرسـال أو إعادة إرسـال أو نشـر بيانات أو معلومات عن طريق الشـبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو الموقع الإلكتروني أو منصـات التواصـل الاجتماعي تنطوي على أخبار كاذبة تسـتهدف الأمن الوطني والسـلم المجتمعي أو ذم أو قدح أو تحقير أي شـخص بالحبس مدة لا تقل عن ثلاثة أشـهر أو بغرامة لا تقل عن (5000) خمسـة آلاف دينار ولا تزيد على (20000) عشـرين ألف دينار أو بكلتا هاتين العقوبتين"[1].

[1] قرار محكمة صلح جزاء عمان رقم 2023/22600 بإدانة المشتكى عليه بجرم نشر ما ينطوي على ذم وقدح وتحقير لإحدى السلطات في الدولة، وذلك بحدود المادة 15 من قانون الجرائم الالكترونية والحكم عليه بالحبس لمدة ثلاثة أشهر والرسوم. تم اسناد جريمة أخرى وهي نشر ما من شأنه إثارة الفتنة أو النعرات أو استهداف السلم المجتمعي أو الحض على الكراهية أو الدعوة الى العنف باستخدام منصة التواصل الاجتماعي وفق أحكام المادة 17 من قانون الجرائم الإلكترونية، إلا أن المحكمة استبعدت هذا الجرم معللة قرارها أنه لا يوجد في منشورات المشتكى عليه أيّ دعوة للتحريض على العنف من أيّ جهة أخرى ولا تحريضاً على أيّ فئة من فئات المجتمع. انظر: https://legal-agenda.com/بلكي-مسؤولينا-صاروا-رجال-عبارة-ذمّ-تح/#_ftnref1
كذلك أصدرت محكمة صلح جزاء عمان القرار رقم 2023/19411 بإدانة المشتكى عليهما بجرم نشر الأخبار الكاذبة وبغرامة 5000 دينار بالإضافة الى الرسوم، حيث تم نشر رسالة صوتية وأخرى مكتوبة تؤكدان على وقوع زلزال في منطقة البحر الميت، وتحذر من حدوث انقطاعات في شبكات الانترنت والهواتف ووسائل الاتصال الأخرى ما اثار الهلع والقلق بين الافراد في المجتمع. انظر: https://www.sarayanews.com/article/879705

كما نصت المادة 21 من قانون الجرائم الالكترونية الأردني على انه: "كل من طلب أو قبل لنفسه، أو لغيره هدية، أو وعداً أو أية منفعة أخرى سواء تم ذلك داخل المملكة أو خارجها لينشر أو يعيد نشر محتوى غير قانوني أو أخباراً زائفة، باستخدام شبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقع إلكتروني أو منصة تواصل اجتماعي يعاقب بالحبس من سنة الى ثلاث سنوات وبغرامة تعادل قيمة ما طلب أو قبل من نقد أو عين على أن لا تقل عن (5000) خمسة آلاف دينار".

وبتحليل هذه النصوص، نستخلص صورتين لجريمة نشر الشائعة او معلومات كاذبة حسب التشريع الأردني، الصورة الأولى: نشر أو إعادة نشر اخبار كاذبة بوسائل إلكترونية.

ويتحقق الركن المادي لهذه الصورة بمجرد نشر أو ارسال او إعادة ارسال معلومات أو بيانات تنطوي على اخبار كاذبة، حيث اشترط المشرع الأردني ان يتم الفعل عن طريق شبكة المعلومات، وذلك بغرض خداع الجمهور أو تضليله أو إحداث اضطراب في التصورات العامة تجاه قضايا معينة. والتي قد تتخذ هذه المعلومات الكاذبة طابعًا سياسيًا أو اقتصاديًا أو اجتماعيًا، مثل نشر إشاعات عن انهيار اقتصادي، أو فساد غير مثبت، أو أخبار مغلوطة عن مؤسسات الدولة أو عن شخصيات عامة.

كما يمكن ان يقع الفعل بإعادة الارسال لهذه الاخبار، أي أن الشخص الذي ارسل الخبر ليس ذات الشخص الذي انشأ او كتب الرسالة المتضمنة للأخبار الكاذبة.

وحسب نص المادة 15 من قانون الجرائم الالكترونية الأردني، اشترط المشرع ان تكون هذه الاخبار الكاذبة تستهدف الأمن الوطني والسلم المجتمعي أو ذم أو قدح أو تحقير لأي شخص، وهو محل جريمة نشر الاخبار الكاذبة بوسائل إلكترونية.

ولا يشترط في هذه الجريمة أن تؤدي المعلومات الكاذبة إلى وقوع ضرر فعلي مباشر حتى يُعاقب عليها، وإنما يكفي أن تكون **من شأنها** التأثير في الرأي العام، أي أن تخلق حالة من القلق أو التشويش أو الفتنة

أو فقدان الثقة في المؤسسات العامة (علي، د.ت.). وذهب بعض الفقه الى القول بأن جريمة الشائعة يمكن أن يحدث الشـــروع فيها، حيث إنه بمجرد بدء الفاعل بالســـلوك، والمتمثل في نشـــر الأخبار والمعلومات والبيانات الكاذبة بقصـــد زعزعة نفســـية الأمة أو النيل من مكانة وهيبة الدولة تتحقق الجريمة في صـــورتها الكاملة، بما يستوجب العقوبة للجريمة التامة، إلا أنه من المتصـور ان يحدث الشـروع فيها، كأن يتم ضـبط الجاني وهو يحاول نشر الشائعات، كأن يتم ضبطه وهو يقوم بطباعة الخبر بقصد نشره (شاكر و دقاني، 2022). واعتبر المشرع الفلسطيني في المادة 49 من القرار بقانون رقم 10 لسنة 2018 كل من شرع في ارتكاب جناية او جنحة من الجرائم المنصـوص عليها في هذا القرار بقانون مرتكباً لجريمة الشـروع ويعاقب بنصف العقوبة المقررة لها.

فالعبرة هي بإحداث "خطر" على الســـلم الاجتماعي أو الاســـتقرار العام. وبالتالي فهي تعتبر من جرائم الخطر، أي إن الجريمة تقوم لمجرد قيام الركن المادي وهو فعل نشـر الخبر الكاذب وقابليته لاحداث نتيجة جرمية أي احتمال وقوع ضرر.

فيما يتعلق بالسببية في القانون الجزائي، فهي مسألة موضوعية بحتة يقدرها قاضـي الموضوع بما يقوم لديه من دلائل وتمثل أن الأثر المترتب على انه لولا الســـلوك المجرم لما وقعت النتيجة أي أن يكون النشـــاط الجزائي الذي يقوم به الجاني في نشـر الاخبار الكاذبة هو السـبب في تحقيق النتيجة الإجرامية وهو تكدير الأمن العام وإلحاق الضـرر بالمصـلحة العامة وأن تكون هذه الأخيرة قد تحققت بسـلوك الجاني بحيث لولاه لما حدثت النتيجة (الفقي، 2020).

الصورة الثانية: طلب أو قبول هدية لغايات نشر أخبار كاذبة.

حيث نصـــت المادة 21 من قانون الجرائم الالكترونية الأردني على انه: "كل من طلب أو قبل لنفســـه، أو لغيره هدية، أو وعداً أو أية منفعة أخرى سواء تم ذلك داخل المملكة أو خارجها لينشر أو يعيد نشر محتوى غير قانوني أو أخباراً زائفة، باســـتخدام شـــبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقع

إلكتروني أو منصـــة تواصـــل اجتماعي..."، فالســـلوك الجرمي هنا يتمثل في قبول الهدية أو الوعد أو أي منفعة من اجل نشر خبر كاذب أو إعادة نشره، فنستنتج ان مجرد قبول الهدية يتحقق السلوك الجرمي دون الحاجة الى اثبات النشر بشكل فعلي (عمايره، 2025).

فيما يتعلق بالركن المعنوي في جريمة نشـر معلومات كاذبة، هو يعد جوهرًا لقيام المسـؤولية الجنائية، وهو الذي يبيّن النية الكامنة وراء الفعل، فالمشـرع الأردني يعاقب كل من يقوم قصـداً بنشـر بيانات كاذبة[1]، أي ان الجاني يعلم أن المعلومات التي يقوم بنشـرها أو ترويجها كاذبة، أو لا تسـتند إلى مصـدر موثوق، ورغم ذلك يقدم على نشرها مع إدراكه لما قد تسببه من اضطراب.

فالقصـد الجنائي المطلوب هو العام والذي يتجلى في إدراك الجاني لمحتوى ما ينشره، وإرادته لإيصـاله إلى الجمهور العام، رغم إدراكه لتأثيره الســـلبي المحتمل. اما فيما يتعلق بالقصـــد الخاص، حيث لا يشـــترط وجوده، فالمشرع في جرائم أمن الدولة جرم الأفعال التي من شأنها ان تلحق الضرر بأمن الدولة ولم يشترط تحقق الخطر بل اكتفى بأن يكون هذا الخطر محتملاً (عالية، 1999). حيث ان اشـتراط القصـد الخاص في هذا النوع من الجرائم قد يفوت على المشـرع مقصـده من الحفاظ على أمن الدولة، وذلك بإفلات كثير من المجرمين من العقوبة، بدعوى أنه لم يكن لديه نيّة الاضرار بالمصالح المذكورة.

فقد يكون القصـد الخاص متمثل في نية الجاني في تضـليل المجتمع، أو إثارة البلبلة، أو تقويض الثقة في المؤسـسـات، أو توجيه الرأي العام نحو موقف معين مخالف للواقع، لأسـباب أيديولوجية أو سـياسـية أو اقتصـادية أو حتى شـخصـية. وقد يُستدل على هذا القصـد من توقيت النشـر (مثلاً نشـر إشـاعة اقتصـادية بالتزامن مع أزمة)، أو من لغة الخطاب المســـتخدمة، أو من تكرار نشـــر معلومات ثبت كذبها، وهذا ما يصعب اثباته.

[1] المادة 15 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

في الواقع العملي في فلسطين، ونظراً لعدم وجود نصوص قانونية صريحة تجرّم نشر الشائعات او الأخبار الكاذبة في قانون الجرائم الالكترونية، يقوم القضاء بالاستناد الى مواد من قانون العقوبات الأردني رقم 16 لسنة 1960 النافذ في الضفة الغربية تعالج جريمة نشر الشائعات والتي ادرجها المشرع بالفصول المتعلقة بالجرائم الواقعة على أمن الدولة.

حيث تناولت المادة 130 منه فعل الدعاية الذي يهدف الى اضعاف الشعور القومي أو إيقاظ النعرات العنصرية وعاقب عليها بالأشغال المؤقتة، وكذلك المادة 131 والذي نص فيها على نفس العقوبة لكل من يذيع انباء يُعرف بأنها كاذبة أو مبالغ فيها ومن شأنها ان تضعف نفسية الأمة. حيث يمكن الاستناد الى هذه المواد لمعالجة حالات نشر الاخبار الكاذبة التي تتم بوسيلة الكترونية والتي تهدف الى تهديد السلم المجتمعي في فلسطين.

ومع ذلك، ترى الباحثة ان هذه النصوص التي يمكن الرجوع اليها في هذا السياق مبهمة وغير واضحة، ولا تزال غير كافية لمواجهة هذا الاعتداء الذي يهدد امن المجتمع وسلمه، حيث ان الوسيلة المستخدمة في هذا الاعتداء تزيد من خطورة الامر لما توفره من إمكانية حدوثه وانتشاره بشكل سريع وعلى نطاق واسع وبالتالي خلق حالة من الفوضى وعدم الاستقرار وهدم نسيج المجتمع. ومن أجل التصدي لهذه الظاهرة، يجب إفراد نصوص تشريعية خاصة تجرّم هذا الفعل، وكذلك ادراج تعريف دقيق للشائعات الالكترونية والتمييز بين صورها وخطورة كل شكل منها، وعلى أساس ذلك، وضع عقوبات رادعة لمرتكبيها تتناسب مع خطورة كل منها. كما يجب تعزيز التعاون بين الجهات الحكومية ومزودي خدمات الإنترنت ومنصات التواصل الاجتماعي لرصد وحذف المحتوى المضلل في اسرع وقت ممكن لتجنب وقوع أية اضطرابات داخلية. كما يجب توعية المواطنين بأهمية التحقق من صحة المعلومات قبل مشاركتها، وتشجيعهم على الاعتماد على المصادر الرسمية والموثوقة. بالإضافة إلى ذلك، يمكن إنشاء وحدات متخصصة داخل الأجهزة الأمنية لرصد ومتابعة الأخبار الكاذبة واتخاذ الإجراءات القانونية اللازمة ضد مروجيها.

كما يجب الإشارة الى ان دخول الذكاء الاصطناعي كعنصر فاعل في بنية التفاعلات الرقمية، جعل من التكنولوجيا الحديثة أداة تُستخدم ليس فقط لأغراض اقتصادية وعلمية، بل أيضًا في تنفيذ أنشطة موجهة تهدف إلى المساس باستقرار الدول وأمنها، والتأثير على الرأي العام الداخلي، وصناعة خطاب رقمي مضلل يصعب تمييزه عن المحتوى الطبيعي.

فعلى الصعيد الفلسطيني، تزداد هذه التحديات وضوحًا، حيث لا تزال البيئة التشريعية غير مهيأة بالكامل لاستيعاب هذه الأنماط الحديثة، إذ إن القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، على الرغم من كونه يمثل خطوة متقدمة نحو بناء إطار قانوني للفضاء الرقمي الا انه لم يتطرق لمعظم الصور الحديثة لهذا النوع من الهجوم.

فالقانون لم يتناول على سبيل المثال إساءة استخدام تقنيات الذكاء الاصطناعي في إنشاء محتوى مضلل أو مزيف يحمل طابعًا سياسيًا يُستخدم في التحريض أو التأثير على الرأي العام، وهي ظواهر باتت متكررة ومؤثرة في البيئة الرقمية الفلسطينية. كما أغفل القانون التهديد المتزايد الناتج عن تداول العملات الرقمية المشفّرة في تمويل نشاطات مشبوهة، قد تشمل دعم جماعات تعمل على زعزعة الأمن الداخلي أو تمويل حملات إعلامية رقمية موجهة تهدف إلى تفكيك الجبهة الداخلية. كذلك، لم يعالج النص التشريعي الفلسطيني مسألة الاختراقات الذكية التي تتم عبر تقنيات التسلل الشبكي المتقدمة، ولا الجرائم التي ترتكب داخل أنظمة التشغيل السحابية التي تعتمدها المؤسسات الحكومية أو الأحزاب السياسية (الخطيب و وآخرون، 2016).

ومن ابرز ما انتجه الذكاء الاصطناعي ما يسمى بالتزييف العميق (Deepfake)

ان التزييف بمفهومه العام هو " إعادة إنتاج أو إعادة تقديم لعمل ما بطريقة غير مشروعة " (Baize, 1999)، إذ هو عملية مادية وصورة من إحدى صور الكذب يقوم بها الشخص بغرض تغيير الحقيقة التي من شأنها الحاق الضرر بالحقوق والمراكز القانونية للأفراد (حجازي، 2002).

ظهر مصـطلح التزييف العميق في نهاية عام 2017، وكان ذلك اسـم لحسـاب (deepfakes)على موقع ريديت، لتركيب صـــور لعدد من المشـــاهير في فيديوهات غير حقيقة (الخولي، 2021)، ويعرّف أليكس أنجلز التزييف العميق بأنه "عبارة عن مقاطع صـــوتية وصـــور وفيديوهات تظهر وكأنها حقيقية لكنها في الواقع اصطناعية تم إنشاؤها باستخدام تقنيات الذكاء الاصطناعي" (Engler, 2019).

يمثل التزييف العميق أحد أخطر تطبيقات الذكاء الاصـطناعي التي تُستخدم لإنتاج فيديوهات أو تسـجيلات صوتية مزيفة لكن تُقدّم للمشاهدين على أنها حقيقية، وقد ثبت أن هذه التقنية قادرة على خداع جمهور واسع بسهولة تامة، فهو نتاج أحد تطبيقات تقنيات الذكاء الاصطناعي التي تسمى نموذج التعليم العميق، ويتكون من صـور حقيقية الى حد كبير، ولا يتلاعب المنتجون الا بعناصـر صـغيرة نسـبياً من الفيديو (مثل تعابير الوجه والصـوت)، مما يسـاهم في واقعية التزييف العميق، وبهذا المعنى يختلف التزييف العميق نوعياً عن الصـور المعدلة بالفوتوشـوب فهو لا يخدع العيون فحسـب، بل يخدع الآذان ايضـاً (Dobber, Metoui, Trilling, Helberger, & Vreese, 2021). فتكمن خطورته في قدرته على خلق أحداث لم تقع، أو نسـب أقوال وأفعال لرموز رسـمية، أو قادة سـياسـيين، مما يؤدي إلى إشـعال الفتن، وتأجيج المشـاعر الجماهيرية، وخلق ردود فعل على وقائع لم تحدث أصلًا.

فلا تقتصـــر جرائم التزييف العميق على إيذاء الأشـــخاص والمؤســـســـات الخاصـــة وإنما تشـــكل خطراً على المجتمع وعلى الدولـة (Hancock & Bailenson, 2021)، كـارتكـاب التزييف العميق ضـــــد رجال الدولة وفي الانتخابات. فمثلاً خلال الانتخابات الامريكية 2020 اتهمت الولايات المتحدة الامريكية روســـيا باســـتخدام تقنية التزييف العميق للإضـــرار بالنظام الديمقراطي والانتخابات في الولايات المتحدة (Chesney & Citron, 2019).

كما ويمكن ان ترتكب جرائم التزييف العميق ضد أمن واستقرار الدولة، كأن تستخدم من قبل قوى اجنبية أو محلية تسعى إلى زعزعة الدولة من خلال بث الفوضـى، أو إثارة النعرات الطائفية سواء في أوقات الحروب

أو السلم، فمثلاً خلال الغزو الروسي لأوكرانيا في عام 2022، ظهر الرئيس الأوكراني فولوديمير زيلينسكي في فيديو مزيف يطالب فيه قواته الاستسلام للروس (Brooks & et al).

في البيئات السياسية المشحونة مثل الحالة الفلسطينية، هذه الأداة الرقمية القوية لا تجد في القانون الفلسطيني أي معالجة صريحة، إذ لا يوجد نص يُجرّم إنتاج محتوى زائف باستخدام الخداع البصري أو السمعي، إذا لم يكن متصلًا بجريمة تقليدية كالاحتيال أو التشهير. وهذا يفتح المجال واسعاً أمام استخدام هذه التقنية في سياقات ذات أبعاد أمنية وسياسية حساسة دون أن تقابل برادع قانوني فعّال. في ظل محدودية الوعي المجتمعي حول كيفية تمييز هذا النوع من المحتوى، تزداد الحاجة إلى أدوات قانونية تلاحق الفعل من لحظة إنتاجه، وليس فقط عند تحقق الضرر، خصوصًا حين يكون هذا الضرر متعلقًا بثقة الناس بمؤسساتهم أو رموزهم السياسية (الحديثي و الزعبي، 2010). فالخطورة في هذا النوع من المحتوى لا تكمن فقط في سرعة انتشاره، بل في واقعيته الشديدة وصعوبة تمييزه من قبل العامة، مما يجعله أداة فعالة لإحداث الانقسام والتشويش.

المطلب الثالث: التلاعب في البيانات الحكومية الحساسة

مع اتساع رقعة التحول الرقمي واعتماد مؤسسات الدولة على النظم الإلكترونية في أرشفة البيانات وإدارة الخدمات، برزت مشكلة التلاعب بالبيانات الحكومية كإحدى أخطر الاعتداءات الإلكترونية التي تهدد الأمن الداخلي للدولة بشكل مباشر. لم يعد استهداف المواقع الحكومية يقتصر على تخريبها أو تعطيلها، بل أصبح يتجاوز ذلك إلى محاولات دقيقة للتلاعب بمحتوى البيانات، حذف معلومات، تغيير محتوى التقارير الرسمية، أو إدخال معلومات مزيفة يمكن أن تستعمل لاحقًا في خلق أزمات سياسية أو اقتصادية أو اجتماعية[1].

[1] تزداد خطورة هذه المسألة في فلسطين بسبب هشاشة البنية التحتية الإلكترونية للمؤسسات الحكومية، وغياب منظومات حماية سيبرانية متكاملة، بالإضافة إلى غياب التشريعات التفصيلية التي تُجرّم بشكل صريح التلاعب في البيانات الحكومية، وليس فقط اختراق الأنظمة. كما أن بعض حالات التلاعب قد لا تُكتشف إلا بعد فترة طويلة، عندما تكون الأضرار قد وقعت، وتكون المعلومات المزيفة قد استُخدمت لأغراض سياسية أو إعلامية أو حتى لتمرير قرارات

تمثل البيانات الحكومية الحساسة عصب الإدارة العامة للدولة، وتغطي طيفاً واسعاً من المجالات، بدءاً من بيانات المواطنين، وصولًا إلى الملفات الأمنية والاقتصادية والصحية وغيرها. فالاعتداء عليها يفتح الباب أمام سيناريوهات كارثية، مثل ما حدث في المغرب من اختراق لقاعدة بيانات مغربية وتسريب بيانات حساسة (الجزيرة، 2025)، أو كما حدث في سوريا من تسريب واسع النطاق لبيانات من مواقع حكومية سورية، والتي من ابرزها موقع وزارة الصحة ووزارة الشؤون الاجتماعية، حيث تضمن التسريب بيانات شخصية ووثائق رسمية (اكثر من 140 صورة لجوازات سفر سورية حقيقية)، وبطاقات شخصية، ووثائق عسكرية وسجلات تجنيد، وتم عرض المحتوى للبيع في الدارك ويب (فريق المركز السوري للأمن الرقمي، 2025). أو العبث بسجلات الناخبين قبيل الانتخابات، أو التأثير على قرارات سياسية مبنية على بيانات خاطئة.

فتتعاظم خطورة هذا النوع من الاعتداءات نظرًا لضعف البنية التحتية التكنولوجية في بعض المؤسسات، وانخفاض مستوى الحماية السيبرانية، إضافة إلى التداخلات السياسية والأمنية المعقدة التي تجعل بعض الجهات تسعى لاختراق هذا النوع من البيانات (Pfleeger, Pfleeger, & Margulies, 2015).

من الناحية القانونية، لم تقم التشريعات العربية بتعريف مصطلح "التلاعب بالبيانات" بشكل مباشر، لكنها أدرجت الأفعال التي تنطوي على ذلك، والتي تضمن ادخال او اتلاف او حذف او تغيير او افشاء لبيانات غير متاحة للكافة.

ويختلف التلاعب عن فعل الدخول غير المصرح به بأن الأخير لا يتطلب وقوع ضرر جراء حصوله، بل يكفي لوقوع الجريمة مجرد الولوج دون اذن الى نظام معلوماتية او شبكة الكترونية، اما التلاعب فيشترط ان

داخلية تحت غطاء بيانات مغلوطة. ويصبح هذا الأمر أكثر تعقيدًا حين يتم تنفيذ الاعتداء من خارج البلاد أو عبر أدوات تقنية يصعب تتبعها محليا، ما يضع مؤسسات الدولة أمام أزمة حقيقية في الاستجابة.

يوقع تغييرا على البيانات المخزنة في ذلك النظام، فبالتالي يتطلب قصداً جنائياً خاصاً وهذا ما سنتناوله لاحقاً.

وترى الباحثة انه يمكن تعريف مصطلح التلاعب بالبيانات على انه: كل تدخل متعمد في البيانات أو المعلومات، المخزّنة الكترونياً، سواء عن طريق الحذف او الإضافة او التعديل او الاخفاء، ويهدف هذا التدخل الى تغيير حقيقة البيانات لإلحاق الضرر بالآخرين، سواء على مستوى الفرد او المصلحة العامة.

لا يوجد في القانون الفلسطيني الحالي نصوص تفصيلية تجرّم التلاعب في البيانات الحكومية الرقمية بشكل دقيق، بل يتم التعامل معها ضمن إطار عام يتعلق بـ " "الدخول غير المشروع" وهو مصطلح لا يكفي لتغطية حالات التلاعب التي قد تتم من داخل المؤسسات نفسها أو عبر اختراقات متقدمة. فيتم اللجوء لنص المادة 4 من القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018 لتغطية حالات التلاعب، والتي تتحدث بشكل أساسي عن جريمة الدخول غير المشروع وما يترتب عليه من تلاعب في البيانات كنتيجة للفعل المجرم "الدخول غير المصرح به"، وهو ما سنوضحه في هذا المطلب.

بالمقارنة مع بعض الأنظمة القانونية العربية، مثل القانون المصري لمكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، نجد نصوصًا محددة تجرّم التلاعب في البيانات الحكومية، وتضع عقوبات مغلظة لذلك النوع من الأفعال[1]، خاصة إذا ترتب عليها تهديد للأمن القومي أو الإضرار بالمصالح العليا للدولة حيث جاء في نص المادة 34 منه " اذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الاخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي، تكون العقوبة السجن المشدد". والقانون

[1] انظر نص المادة 20 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018.

الأردني كذلك تعامل مع هذه المسألة وخصص لها نصوص كافية لتجريمها وتناول فيها القصد الجرمي للجاني كما وعاقب على الشروع فيها بالعقوبة المقررة للجرائم ذاتها[1].

ولعل من اكثر التشريعات التي تناولت أفعال التلاعب بالبيانات الحكومية التشريع الاماراتي حيث افرد عدد من النصوص التي تضمنت احكام تتعلق باختراق الأنظمة المعلوماتية الخاصة بالدولة، والاضرار بأنظمتها المعلوماتية وكذلك الاعتداء على البيانات والمعلومات الحكومية.

استفاض المشرع الاماراتي في موضوع الهجمات الإلكترونية على البنية التحتية للدولة فأفرد عدداً من النصوص في المرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية رقم 34 لسنة 2021 تتناول أنواع الاعتداء الذي قد يحدث لهده المعلومات. حيث فرّق المشرع الإماراتي ما بين فعل الاختراق (الدخول غير المشروع) وما بين التلاعب والإضرار بالبيانات، فادرج تعريفاً شاملاً للاختراق في المادة الأولى منه، ووضح في نفس المادة مفهوم الهجمات الالكترونية على انها " كل استهداف متعمد ومخطط للأنظمة المعلوماتية أو البنية التحتية أو الشبكات الالكترونية أو وسائل تقنية المعلومات يقلل من قدرات ووظائف أي منها، سواء كان ذلك لغرض شخصي أو لأغراض الاعتراض أو التسلل أو الاختراق أو التسريب أو بغرض تعريض البيانات أو المعلومات للخطر أو تعطيل العمليات وما في حكمها." (مرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية رقم 34 لسنة 2021).

حيث تناول المشرع الامارتي التلاعب بالبيانات في اكثر من مادة من المرسوم، تارة كنتيجة مترتبة على فعل الاختراق (الدخول غير المشروع)، وتارة أخرى كصورة مستقلة تتطلب قصد خاص.

تتعلق المادة 3 من المرسوم باختراق أنظمة معلوماتية خاصة بمؤسسات الدولة، ففي الفقرة الأولى منها حدد المشرع السلوك الاجرامي الذي يمثل جريمة الاختراق وهو الدخول غير المشروع، وفي الفقرة الثانية من

[1] انظر المادة 4 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

ذات المادة تناول احكام تتعلق بالإضـــرار او التدمير او التعطيل للنظام المعلوماتي التابع للمؤســـســـات الحكومية كنتيجة للسلوك الجرمي الواقع (الاختراق) وشدد العقوبة على ذلك، بينما الفقرة الثالثة جاءت بحكم خاص بجريمة الاختراق، وذلك اذا كان الاختراق لغرض الحصول على معلومات، فتضمنت عقوبة مشددة لا تقل عن 7 سنوات وغرامة لا تقل عن 250000 درهم اذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بمؤسسات الدولة[1].

اما في المادة 5 من المرسوم عاقب بالسجن المؤقت والغرامة لكل من تسبب عمداً بالإضرار او التدمير او إيقاف او تعطيل موقع إلكتروني أو نظام معلوماتي أو شبكة معلوماتية عائدة لمؤسسات الدولة.

وفي المادة 7 من المرسوم تناول احكاماً خاصة بالاعتداء على البيانات والمعلومات الحكومية وشدد العقوبة بما يتناسب مع خطورة الفعل وكذلك حجم الضرر، حيث نصت على (المرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية، 2021):

1. "يعاقب بالسجن المؤقت مدة لا تقل عن 7 سنوات والغرامة لا تقل عن (500000) خمسمائة ألف درهم ولا تزيد على (3000000) ثلاثة ملايين درهم كل من حصل أو استحوذ أو عدل أو أتلف أو أفشى أو سرب أو ألغى أو حذف أو نسخ أو نشر أو أعاد نشر بغير تصريح بيانات أو معلومات حكومية سرية.

[1] المادة (3) من المرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية رقم 34 لسنة 2021
اختراق الأنظمة المعلوماتية الخاصة بمؤسسات الدولة
1- يعاقب بالسجن المؤقت والغرامة التي لا تقل عن (200,000) مائتي ألف درهم ولا تزيد على (500,000) خمسمائة ألف درهم، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات عائدة لمؤسسات الدولة .
2- وتكون العقوبة السجن مدة لا تقل عن (5) خمس سنوات والغرامة التي لا تقل عن (250,000) مائتين وخمسين ألف درهم ولا تزيد على (1,500,000) مليون وخمسمائة ألف درهم، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أي بيانات أو معلومات أو خسارة سريتها أو وقعت الجريمة نتيجة لهجمة إلكترونية.
3- وتكون العقوبة السجن مدة لا تقل عن (7) سنوات والغرامة التي لا تقل عن (250,000) مائتين وخمسين ألف درهم ولا تزيد على (1,500,000) مليون وخمسمائة ألف درهم، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات الخاصة بتلك الجهات المنصوص عليها بالفقرة الأولى من هذه المادة.

2. وتكون العقوبة السجن المؤقت مدة لا تقل عن 10 سنوات والغرامة لا تقل عن (500000) خمسمائة ألف درهم ولا تزيد على (5000000) خمسة ملايين درهم إذا ترتب على الأفعال المنصوص عليها بالند (1) من هذه المادة أضراراً للدولة، أو اذا ترتب عليها فقدان سرية عمل الأنظمة والبرمجيات الإلكترونية الخاصة بالمنشآت العسكرية والأمنية وما يتعلق بالاتصال ونقل المعلومات السرية.

3. ويعاقب بالسجن المؤقت كل من تلقى أي من البيانات والمعلومات المشار اليها بالبند (1) من هذه المادة، واحتفظ بها أو خزنها أو قبل التعامل بها أو استخدامها رغم علمه بعدم مشروعية الحصول عليها".

يتجسد الركن المادي لجريمة التلاعب في البيانات الحكومية في كل سلوك مادي يمس سلامة أو صحة أو مصداقية البيانات الرسمية المخزنة في النظم الإلكترونية التابعة للجهات الحكومية، أو المتداولة فيما بينها. وقد يأخذ هذا السلوك صورًا متعددة، منها: إدخال بيانات خاطئة عمدًا في نظام حكومي، تعديل معلومات موجودة دون ترخيص، حذف معلومات مهمة بهدف التستر أو التشويه، أو اختراق أنظمة إلكترونية رسمية للوصول إلى بيانات وتغييرها أو تعطيلها.

يتطلب تحقق الركن المعنوي في هذه الجريمة توافر القصد الجنائي العام، والمتمثل في علم الجاني بأن البيانات التي يتعامل معها هي بيانات حكومية حساسة، وأن التغيير الذي يقوم به غير مشروع ومخالف للقانون، مع إرادة واضحة في تنفيذ هذا السلوك. ويتعين أن يكون الجاني مدركًا لخطورة فعله على مؤسسات الدولة أو على المصلحة العامة. أما **القصد الجنائي الخاص**، فيتحقق عندما يكون الجاني قد سعى من خلال فعله إلى تحقيق غرض معين، كتشويه صورة الحكومة.

جاء المشرع الفلسطيني في المادة 4 من القرار بقانون بشأن الجرائم الالكترونية بما يجرم فعل الولوج الى نظام معلوماتي عمداً او تجاوزاً لدخول مصرح به أو استمر بالتواجد بها بعد علمه بذلك، وشدد عقوبة هذا الفعل في حال وقع على بيانات حكومية.

فيما يتعلق بالركن المعنوي لجريمة الدخول غير المشروع بصورتها البسيطة لا يشترط توافر القصد الجنائي الخاص، انما يكفي توفر إرادة الفاعل الى الولوج عمداً او تجاوز الدخول المصرح به، او استمراره بالتواجد بعد علمه بذلك. ويرى جانب من الفقه الى ان الدخول الى النظام يكون مشـــروعاً إذا كان دخوله نتيجة الصدفة أو الخطأ، فإذا دخل الشخص لمكان فجأة فعليه الخروج وهو ما يطلق عليه اسم مصطلح "حسن النية"، وإذا بقي في داخل النظام فيكون توافر بحقه القصـــد الجنائي العام الذي تقوم عليه الجريمة وهو ما نطلق عليه اسم مصطلح "سيء النية" (رمضان، 2001).

وتطرق ايضـــاً في الفقرة الثالثة من ذات المادة الى ما يمكن ان يترتب على فعل الولوج لنظام معلوماتي حيث نص على " اذا ترتب على هذا الدخول إلغاء بيانات أو معلومات الكترونية في النظام المعلوماتي أو حذفها أو اضـــافتها أو إفشـــاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نســـخها أو نشـــرها أو اعادة نشرها..... يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار اردني ولا تزيد على ثلاثة آلاف دينار اردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين".

كما وشدد هذه العقوبة في حال ترتب ما ذكر في الفقرة الثالثة على بيانات حكومية، لتصبح جناية (السجن مدة لا تزيد على خمس ســنوات) و غرامة لا تقل عن ثلاثة الاف دينار اردني ولا تزيد على خمســة آلاف دينار اردني.

فيلاحظ ان المشرع الفلسطيني شدد العقوبة هنا اذا نتج عن فعل الدخول غير المشروع ضرر، واعتبرها من الجنايات اذا كان هذا الضرر واقع على بيانات حكومية.

وترى الباحثة إن فلسطين بحاجة إلى صياغة قانونية جديدة تأخذ بعين الاعتبار الطبيعة الخاصة للبيانات الحكومية، وتفصـــل بين الدخول غير المشـــروع والتلاعب المتعمد بالبيانات من داخل النظام نفســـه، وتُفرد عقوبات تتناسب مع الأثر الخطير لهذه الأفعال على الأمن الوطني. كما يجب تطوير البنية التقنية لحماية

قواعد البيانات الحكومية، وتعزيز دور وحدة الجرائم الإلكترونية في مراقبة ومعالجة الاختراقات فور وقوعها، مع توفير أدوات رقمية حديثة لرصد التعديلات غير المرخصة وتحليلها قانونيًا بشكل سريع وفعال.

المطلب الرابع: الارهاب الالكتروني وصوره

لطالما كان الارهاب ولا زال من اخطر الظواهر التي تهدد سلم وامن المجتمعات على مر العصور، فهي ظاهرة قديمة، لكنها تتجدد وتتطور بتطور المجتمعات، فازدادت خطورة نظراً لاتساع نطاق استخدام التكنولوجيا في العالم، حيث تشكل هذه التكنولوجيا ارضاً خصبة للاعمال الارهابية، لما توفر امكانياتها من التحرك بمرونة عالية وكفاءة في الانجاز، فأصبحت شبكات الانترنت منبراً للارهابيين في نشر الارهاب والعنف ووسيلة للاتصال بينهم.

يعرّف الارهاب بأنه الاستخدام العمدي والمنظم لوسائل من طبعها إثارة الرعب والفزع بقصد تحقيق بعض الأهداف (عبد الهادي، 1986). ويعرّف ايضاً بأنه اسلوب عنيف للمعارضة السياسية وهو يتكون من العنف والتهديد به، وقد يتضمن التهديد او العنف البدني الحديدي، وقد يمارس العنف ضد أبرياء أو ضد أهداف لها ارتباط مباشر بالقضية التي يعمل بها الارهابيون من أجلها (النوايسة ع.، 2005).

اما الاتفاقية العربية لمكافحة الارهاب الصادرة من مجلس وزراء الداخلية العرب بالقاهرة في سنة 1998 فقد عرّفت الارهاب بأنه: كل فعل من افعال العنف أو التهديد به أياً كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروع اجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم او حريتهم او امنهم للخطر او إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض أحد الموارد الوطنية للخطر[1](الاتفاقية العربية لمكافحة الإرهاب، 1998، م2).

[1] المادة (2) من الاتفاقية العربية لمكافحة الارهاب لسنة 1998.

فنستنتج ان الارهاب هو عدوان غير مبرر، يكون مدفوعاً اما بأهداف شخصية او سياسية او دينية، بهدف ترويع الآمنين وتعريض سلامة المجتمع ككل للخطر.

وبالرجوع لقانون العقوبات الاردني رقم 16 لسنة 1960 الساري في الضفة الغربية، فقد عرّف الاعمال الارهابية في المادة 147 بأنها جميع الأفعال التي ترمي إلى إيجاد حالة ذعر وترتكب بوسائل كالأدوات المتفجرة، والمواد الملتهبة والمنتجات السامة أو المحرقة، والعوامل الوبائية، أو الجرثومية، التي من شأنها أن تحدث خطراً عاماً.

اما فيما يتعلق بمفهوم الإرهاب الالكتروني حيث لم يرد في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية ما يعرّفه، شأنه شأن معظم التشريعات والتي اقتصرت على بيان الأفعال التي تعتبر في حكم الاعمال الإرهابية.

وفي ظل غياب تعريف موحد للإرهاب الالكتروني، تعددت التعريفات الفقهية بشأنه، وذلك نتيجة لحداثة المفهوم وايضا لتعدد التعريفات حول مفهوم الارهاب في حد ذاته، فمنهم من عرّف الارهاب الالكتروني بأنه العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الافراد على الانسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد (عطية، 2014). حيث يعتبر هذا التعريف ان الإرهاب الالكتروني هو ذاته الإرهاب التقليدي لكن ما يميّزه عنه الوسيلة المستخدمة وهي الفضاء الالكتروني.

ومنهم من عرّفه بأنه استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو اقتصادية أو أمنية أو عرقية أو دينية (الزنط، 2010)، حيث اعتبر ان الإرهاب الالكتروني قد يستخدم الفضاء الالكتروني كأداة لجريمته وكذلك أيضا كهدف او كمحل للجريمة نفسها.

حيث ترى الباحثة من خلال ما تقدم ان الإرهاب الالكتروني قد يكون: ارهاباً بالمفهوم التقليدي يتم بوسائل الكترونية، حيث تستخدم الجماعات الإرهابية الفضاء الالكتروني في تنفيذ هجماتها، أو قد يكون الفضاء الالكتروني ذاته هو الهدف للجماعات الإرهابية.

وفيما يتعلق بأركان جريمة الإرهاب الالكتروني:

حيث يتكون الركن المادي في أية جريمة من ثلاثة عناصر رئيسية وهي السلوك الاجرامي وهو النشاط المادي الظاهر والذي يصدر عن الجاني، وما يترتب عليه من نتيجة جرمية، ومن ثم وجود علاقة سببية بين النشاط والنتيجة.

ولأهمية النشاط الجرمي في هذا النوع من الجرائم ولما يتميز به الإرهاب الالكتروني عن التقليدي من حيث الوسيلة والمكان، يجعل ذلك من الركن المادي له اكثر من صورة. فعند الحديث عن السلوك الجرمي للإرهاب التقليدي نرى انه يتكون من مجموعة من الأفعال كاستعمال أدوات (كالأدوات المتفجرة) ومواد تشكل خطراً عاماً أو انها تثير الذعر العام، أو التهديد باستخدامها او احداث ضرر جسيم من خلالها، حسب ما جاء في قانون العقوبات النافذ، وقد جاءت هذه الوسائل على سبيل المثال، أي معنى كل فعل من شأنه ان يشكل خطراً عاماً او يثير الذعر بأي وسيلة يعتبر ارهاباً.

أما بالنسبة للركن المادي في الإرهاب الالكتروني، شأنه شأن الركن المادي في أي جريمة معلوماتية، عبارة عن سلوك يتم من خلال الكمبيوتر، أو باستخدام المعالجة الآلية للبيانات (إبراهيم، الجرائم المعلوماتية، 2009).

وتجد الباحثة تعدد في ما يمكن ان يُشكل السلوك الجرمي للإرهاب الالكتروني، حيث يتضمن مجموعة من الأفعال التي يستخدمها الارهابيون في الفضاء الالكتروني، كاستخدامهم للشبكة المعلوماتية لبث الأفكار الإرهابية، او انشاء المواقع الالكترونية لتسهيل القيام بالأعمال الإرهابية او استخدامها في التعبئة الفكرية والتجنيد لصالح هذه الجماعات. او شن هجوم الكتروني على البنى التحتية للشبكة المعلوماتية بقصد

تدميرها وتوقفها عن العمل، مما يحدث آثار مادية واقتصـــادية خطيرة فقد تؤدي هذه الاعمال الى توقف الحكومات الالكترونية عن عملها (العجلان، 2008).

اما النتيجة الجرمية في الإرهاب الالكتروني، حيث انه ومن الناحية القانونية تعتبر من جرائم الخطر، اذ لا يتوقف قيامها على تحقق الضـرر وانما يكفي ارتكاب السلوك المحدد في النصـوص القانونية لتقوم الجريمة ويُعاقب مرتكبها.

لم يتطرق المشـرع الفلسـطيني لظاهرة الإرهاب الالكتروني في قانون الجرائم الالكترونية النافذ، تاركاً الامر للنصـــوص التقليدية في قانون العقوبات التي تتعلق بالإرهاب التقليدي. بالمقابل نرى بالتشـــريع الأردني المقارن تناول موضـوع الإرهاب في قانون مسـتقل وهو قانون منع الإرهاب رقم 55 لسـنة 2006، وتناولت بعض نصوصه احكاماً للإرهاب الذي يتم عبر الشبكة المعلوماتية، حيث نصت المادة 3 منه على " تعتبر الاعمال التالية في حكم الاعمال الإرهابية المحظورة:

اسـتخدام نظام المعلومات أو الشـبكة المعلوماتية أو أي وسـيلة نشـر أو إعلام أو إنشـاء موقع إلكتروني لتسـهيل القيام بأعمال إرهابية او دعم لجماعة أو تنظيم أو جمعية تقوم بأعمال إرهابية أو الترويج لأفكارها أو تمويلها أو القيام بأي عمل من شـــأنه تعريض الأردنيين أو ممتلكاتهم لخطر أعمال عدائية أو انتقامية تقع عليهم".

كما وغلّظ عقوبة الفعل حيث عاقب عليه بالأشـغال الشـاقة المؤقتة (قانون منع الإرهاب الأردني رقم 55 لسنة 2006، المادة 7/ج).

مما سبق، نستنتج بأن الإرهاب عبر الانترنت يتجاوز حدود الجريمة الواحدة او الوصف الجرمي الواحد، إذ توصف بأنها جريمة إرهابية كل جريمة تؤدي الى نشر الذعر او الاخلال بأمن الدولة وزعزعة استقراره.

وبما أن السـلوك الاجرامي لجريمة الإرهاب الالكتروني يتطلب وجود بيئة رقمية واتصـال بشـبكة الانترنت، قام جانب من الفقه بتحديد ابرز صور الإرهاب الالكتروني بما يتماشى مع التقدم التكنولوجي والتي منها:

- إنشاء مواقع إلكترونية إرهابية.
- تدمير المواقع والبيانات والأنظمة الالكترونية.
- التهديد والترويع الالكتروني.
- شن الهجمات الإلكترونية.
- التجسس الإلكتروني.
- تمويل الإرهاب عبر الانترنت.

وسنوضح كل صورة بشكل منفرد.

الفرع الاول: انشاء مواقع الكترونية إرهابية

تتيح المواقع الالكترونية والتواصل الاجتماعي للمستخدمين التواصل في أي وقت وفي أي مكان في العالم، فهي شبكات تفاعلية تنتشر بسرعة فائقة وعلى نطاق واسع، الشيء الذي يجعل من تأثيراتها عابرة للحدود في وقت قياسي، مما يزيد من كثافة وسرعة التحركات والتفاعلات العالمية.

فيمكن لأي تفاعل يحدث في أي جزء من العالم ان يكون له عواقب على أجزاء أخرى من العالم، وهذا ما شكل ارضاً خصبة للجماعات الارهابية في تحقيق مسعاها، بحيث تسمح هذه التقنية للجماعات الإرهابية بالاعتماد ليس فقط على القوة العسـكرية لتحقيق أهدافها، ولكن أيضًـا باللجوء الى الإنترنت والمواقع الإلكترونية لنشـر أفكارها ومعتقداتها المتطرفة وتحركاتها على نطاق واسـع، وايضـا لكسـب الدعم المادي والمعنوي من خلالها.

وعرّف القرار بقانون رقم 10 لسـنة 2018 بشـأن الجرائم الالكترونية في المادة 1 الموقع الالكتروني بأنه " مكان اتاحة المعلومات أو الخدمات على الشبكة الالكترونية من خلال عنوان محدد".

اذ يمكن القول بأن المواقع الالكترونية اداة بالغة الاهمية بالنسـبة للتنظيمات الارهابية فيما يتعلق بالحشـد الفكري او اتخاذ ادواراً اسـتخباراتية للكشـف عن طبيعة الاشـخاص الذين يزورون مواقعهم، والذي يمكّن الجماعات الارهابية من معرفة كيفية استقطاب الاشخاص وبالتالي تجنيدهم، فالموقع الالكتروني عبارة عن عنوان الكتروني، او صفحات الكترونية تحتوي على معلومات معينة تتشكل بواسطة مصمم هذه الصفحة، حيث تقوم الجماعات الارهابية في انشاء وتصميم مواقع الكترونية على شبكة الانترنت من اجل الوصـول الى اكبر شريحة من الناس للتأثير عليهم فكرياً استعداداً لتجنيدهم، او الاستفادة منهم مالياً، او تعليم الافراد كيفية صـناعة المتفجرات او كيفية اختراق المواقع الالكترونية وتدميرها، فهي بمثابة المقر الافتراضـي لها، وقد يكون الهدف من انشاء هذه المواقع ايضا التأثير على الأمن السياسي والعسكري والاقتصادي.

ويمكن تعريف التجنيد على انه " يتمثل في جمع الأشـخاص واسـتقطابهم أو بالأحرى اسـتخدامهم (ترغيباً وترهيباً) للانضـمام إلى العناصـر والجماعات الإجرامية المحلية والدولية في مختلف المجالات، وإعدادهم مادياً ومعنوياً للعمل في خدمة هذه العناصـر والجماعات، والانخراط في أنشـطتها غير المشـروعة وتكليفهم بالقيام بمختلف الأعمال التي تخدم مصالحها وتحقق أهدافها (ابن سليمان، 2013).

فمن خلال شـبكات المعلومات، تقوم المنظمات الإرهابية بتشـكيل قاعدة أيديولوجية بين من لديهم ميل أو استعداد للانخراط في أعمال تدميرية أو تخريبية، مما يوفر قاعدة من الأشخاص ذوي التفكير المماثل الذين يمكن تجنيدهم بسهولة للقيام بأنشطة إرهابية في المستقبل.

كما وقد سـاهم تطور التكنولوجيا في جعل وجود الإرهابيين على الإنترنت متنوعًا ومراوغًا لدرجة أن الموقع الإرهابي يمكن أن يظهر اليوم ويغير عنوانه سـريعًا في الغد، ويختفي ثم يظهر مرة أخرى بعنوان جديد وتصميم مختلف، الأمر الذي يجعل من ملاحقة وتعقب الارهابيين صعباً.

ومن الامثلة على بعض المواقع الالكترونية العربية التي قام بإنشائها وتصميمها بعض التنظيمات الارهابية ما يأتي (زهران، 2019):

- موقع النداء: وهو الموقع الرسمي لتنظيم القاعدة بعد أحداث الحادي عشر من سبتمبر عام 2001م، ومن خلاله تصدر البيانات الإعلامية للقاعدة.
- ذروة السنام: وهي صحيفة إلكترونية دورية للقسم الإعلامي لتنظيم القاعدة.
- صوت الجهاد: وهي مجلة نصف شهرية، يصدرها ما يسمى بتنظيم القاعدة في جزيرة العرب، وهي تصدر بصيغتي وورد، بي، دي، اف (تتضمن مجموعة من البيانات والحوارات مع قادة التنظيم ومنظريه).
- البتار: وهي مجلة عسكرية إلكترونية متخصصة، تصدر عن تنظيم القاعدة، وتختص بالمعلومات العسكرية والميدانية والتجنيد.

الفرع الثاني: تدمير المواقع والبيانات والأنظمة الالكترونية

تتمثل هذه الصورة في قيام الإرهابيين والمنظمات الإرهابية بالقيام بهجمات من خلال شبكة الانترنت، تستهدف تدمير المواقع والبيانات والنظم الالكترونية المتعلقة بالمؤسسات العامة والخاصة وإلحاق الضرر بالبنى التحتية وتدميرها، وهذا من خلال الدخول غير المشروع التي تكون متصلة بشبكة الانترنت أو ما يعرف بنظام PC serveur بهدف تخريب أو تعطيل نقطة الاتصال أو النظام (خميخم، 2020).

حيث ان هذه الصورة تشمل أولا الدخول الى المواقع الالكترونية وهو فعلاً مجرماً بحد ذاته، فبإسقاط هذه الصورة على القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية، نرى انه تناول فكرة الدخول غير المشروع لنظام او موقع الكتروني في المادة 4 منه، او تجاوز الدخول المصرح به بعد علمه بذلك، وتناول ايضا بالفقرة الثانية الدخول غير المشروع لكل ما يتعلق بالبيانات الحكومية. لكن لم يتطرق لفعل "التدمير" للمواقع والأنظمة المعلوماتية.

وبالحديث عن فعل التدمير فهو يعني الحاق الضـــرر بالمنظومة المعلوماتية وهذا يكون بتعطيل الموقع او إيقافه عن العمل او كل ما يلحق الأذى بشكل كامل بالبنية التحتية. وعند الرجوع لنص المادة 4 من القرار بقانون الفقرة الثالثة: "اذا ترتب على هذا الدخول إلغاء بيانات أو معلومات الكترونية في النظام المعلوماتي أو حذفها أو اضـافتها أو إفشـاؤها أو إتلافها أو تغييرها أو نقلها أو التقاطها أو نسـخها أو نشـرها أو اعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني، أو إلغاؤه...".

فالإتلاف والإلغاء يعني تدميراً كلياً للموقع المستهدف بحيث يصبح خارج عن الخدمة.

ترى الباحثة انه كان من الاجدر للمشرع الفلسطيني وضـع نصـوص اكثر ايضـاحاً تنظم فكرة الدخول غير المشـــروع وتحديد الأفعال التي تشـــكل تدميراً للبيانات والأنظمة المعلوماتية وخاصـــة تلك المتعلقة بالدولة لأهميتها وخطورة المســـاس بها وكذلك الافعال التي تدخل في نطاق التلاعب بها ووضـــع عقوبات رادعة تتناسب مع خطورة كل منها.

ففي المادة 6 من القرار بقانون بشـــأن الجرائم الالكترونية عاقب فيها كل من ينتج أو يدخل عن طريق الشـبكة الالكترونية ما من شـأنه أن يوقف العمل أو يعطّل ويتلف البرامج، وحدد العقوبة بالسـجن لمدة لا تزيد على 5 سنوات، وهذا النص جاء عاماً وغير واضح فعلياً

وهنا وجب علينا التطرق للتشريع الأردني، فبالمقارنة مع المادة 4 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023 والتي تنص على:

"أ- يعاقب كل من دخل أو وصـل دون تصـريح أو بما يخالف أو يجاوز التصـريح إلى الشـبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو أي جزء منها يعود للوزارات أو الدوائر الحكومية أو المؤسـسـات الرسمية العامة أو المؤسسات العامة أو الأمنية أو المالية أو المصرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة واطلع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السـلامة العامة أو الاقتصـاد الوطني بالحبس مدة لا

تقل عن ستة أشهر ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن (2500) ألفين وخمسمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار".

وبتحليل الفقرة أعلاه فهي تتحدث عن الدخول غير المشروع إلى الشبكة المعلوماتية أو نظام المعلومات أو تقنية المعلومات الخاصـــة بالجهات الحكومية أو الأمنية أو البنى التحتية الحرجة. والبنى التحتية الحرجة هي مجموعة الأنظمة والشبكات الالكترونية والأصول المادية وغير المادية أو الأصول السيبرانية والأنظمة وتقنية المعلومات التي يعد تشغيلها المستمر ضرورة لضمان أمن الدولة أو اقتصادها أو سلامة المجتمع[1]، أي ان اختراقها يعني اختراق الأســاس التقني الذي تعتمد عليه الدولة في إدارة بياناتها والذي يشـكل تهديداً مباشراً لأمنها القومي.

فالســـلوك الجرمي في الفقرة (أ) متمثل بالدخول غير المشـــروع للشـــبكة واطلع كنتيجة لهذا الدخول او الوصول، على بيانات تمس الامن الوطني او السلامة العامة، وبالتالي تترتب العقوبة والتي حبس وغرامة.

اما الفقرة التي تليها " ب– اذا كان الدخول أو الوصول المنصوص عليه في الفقرة (أ) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نســـخها أو نشـــرها أو إعادة نشرها أو خسارة سريتها أو تشفيرها أو حذفها أو إضافتها أو حجبها أو إفشائها أو التقاطها فيعاقب الفاعل بالأشـغال المؤقتة وبغرامة لا تقل عن (5000) خمسـة آلاف دينار ولا تزيد على (25000) خمسـة وعشـرين ألف دينار، ويعاقب بالأشـغال المؤقتة مدة لا تقل عن خمس سـنوات والغرامة (25000) خمسـة وعشرين ألف دينار اذا تمكن من تحقيق النتيجة".

حيث وضـحت القصـد الجرمي في الشـق الأول فاذا كان الدخول غير المشـروع او الوصـول بما يخالف التصـريح للبيانات الموجودة على الشـبكة المعلوماتية وذلك بغرض تدميرها أو إلحاق الضـرر فيها بالطريقة

[1] المادة 1 من قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

التي نص عليها المشـــرع، يتحول الفعل من جنحة الى جناية معاقب عليها بالأشـــغال المؤقتة مع الغرامة المحددة، فإذا تمكن الفاعل من تحقيق النتيجة وهي الحاق الضـرر بالبيانات والمساس بسـلامة وأمن النظام يكون الحد الأدنى للأشغال المؤقتة 5 سنوات والغرامة بحدها الأعلى.

اما الفقرة ج من ذات المادة، خصـصـت محل الجريمة وذكرت مصـطلح (موقع إلكتروني) "ج- يعاقب كل من دخل أو وصـل قصـداً إلى موقع إلكتروني يعود للوزارات أو الدوائر الحكومية أو المؤسـسـات الرسـمية العامة أو المؤسسات العامة أو الأمنية أو المالية أو المصـرفية أو الشركات التي تملكها أو تساهم بها أي من تلك الجهات أو البنى التحتية الحرجة بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية للمملكة أو السـلامة العامة أو الاقتصـاد الوطني بالحبس مدة لا تقل عن أربعة أشـهر ولا تزيد على ثلاث سـنوات وبغرامة لا تقل عن (2500) ألفين وخمسـمائة دينار ولا تزيد على (25000) خمسة وعشرين ألف دينار".

حيث ان اختراق موقعاً معيناً لا يعني السـيطرة الكاملة على الأنظمة الداخلية للجهة المسـتهدفة، وانما غالباً ما تستهدف خدمات الدولة الالكترونية في ذلك الموقع أو البيانات الحساسة التي يحتويها.

د- اذا كان الدخول أو الوصـــول المنصـــوص عليه في الفقرة (ج) من هذه المادة لإلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو تعديلها أو تغييرها أو نقلها أو نسـخها أو حذفها أو اضـافتها أو حجبها أو تشفيرها فيعاقب الفاعل بالأشغال المؤقتة وبغرامة لا تقل عن (5000) خمسة آلاف دينار ولا تزيد على (25000) خمسـة وعشـرين ألف دينار، ويعاقب بالأشـغال المؤقتة مدة لا تقل عن خمس سـنوات وبغرامة (25000) خمسة وعشرين ألف دينار اذا تمكن من تحقيق النتيجة".

حيث شـمل المشـرع الأردني جميع الأفعال التي ترمي الى تدمير البيانات والحاق الضـرر فيها كما وشـدد العقوبة على مرتكبي هذه الأفعال وعاقب على الشـــروع فيها بذات العقوبة المقررة للجرائم ذاتها وهذا بحد ذاته يشكل تطوراً واضحاً في أساليب الحماية ومكافحة الجرائم الالكترونية الواقعة على أمن الدولة.

الفرع الثالث: التهديد والترويع الالكتروني

يمكن تعريف التهديد بشـــكل عام على أنه: "وعيد بأذى يتضـــمن تعبيراً من الجاني يؤثر في نفس وحرية الإرادة لدى المجني عليه بإنزال الأذى عليه أو على شـــخص آخر يهمه" (شـــمس الدين، 2007). وهذا يعني ان أساسه وجود عنصر الترويع والترهيب، وهو ما تقوم عليه ايضاً الجرائم الإرهابية. ومن هنا يأتي الربط بين الإرهاب وكثير من الجرائم التي تعد قائمة بحد ذاتها كالتخريب والاتلاف والقتل والإرهاب عبر الانترنت (ابن يونس، 2004).

تسعى الجماعات الإرهابية الى استخدام وسائل التقنية الحديثة وشبكة المعلومات كمنابر لتمرير رسائل التهديد، معتمدةً في ذلك على أساليب متنوعة تهدف الى بث الرعب وزعزعة الأمن لدى الافراد والمجتمعات والدول.

ويأتي هذا النهج بغرض الضغط على المستهدفين لحملهم على الاستجابة لمطالب تلك الجماعات، أو من اجل الحصول على التمويل الذي يسهم في تعزيز قدراتها وتنميتها.

فمثلاً، يتم استعمال المواقع الإلكترونية من خلال اللجوء الى التهديد والوعيد بقتل شخصية السياسية والدينية ومؤثرة في المجتمعات أو التهديد بتفجير المنشـآت الحيوية والاسـتراتيجية في الدولة أو التهديد بتعطيل أو إتلاف الأنظمة الإلكترونية للمنشـــآت القاعدية وإلحاق الضـــرر والدمار بالشـــبكات الالكترونية والأنظمة المعلوماتية (خميخم، 2020، صفحة 36).

الفرع الرابع: تمويل الارهاب عبر شبكة الانترنت

يتطلب وجود المنظمات الارهابية واســـتمرار عملياتها توافر إمكانات مادية تمكنها من تحقيق اهدافها والتي من اهمها نشر الفكر الارهابي، والدعاية والترغيب في تجنيد الاتباع، وتوفير الاسلحة والمواد التي تتطلبها العمليات الارهابية، وكذلك تنفيذ ما تخطط القيام به، كل ذلك يتطلب توافر مال، فوجود من يدعم المنظمات الارهابية سواء بطريقة مباشرة او غير مباشرة هو اساس ديمومة هذه المنظمات.

يعرّف تمويل الارهاب على انه " عملية تهدف الى امداد الجماعات الارهابية بالأموال والمعدات والأدوات اللازمة لتنفيذ مخططاتهم الإرهابية" (عرفة، 2013)، ويعرّفه آخرون بأنه "تقديم المساعدات المادية، وكذلك الاسلحة بكافة أنواعها والمأوى والمؤن والتدريب ووسائل النقل والاتصال والوثائق لجهات إرهابية داخلية ام خارجية، وكذلك القيام بعمليات مصرفية لمصلحتها واستثمار وغسيل أموالها" (النوايسة ع.، 2005)، أو "بأنه دعم مادي بأي صـــورة يتم تقديمه للأفراد أو المنظمات الارهابية أو التي تدعم الارهاب، وقد يكون مصدره مشروع أو غير مشروع " (الحمادي، 2018).

وعلى الصـــعيد الدولي، عرّفت الاتفاقية الدولية لقمع تمويل الارهاب لعام 1999 في المادة الثانية منها جريمة تمويل الارهاب بأنها: " قيام اي شخص بتقديم الأموال او جمعها بأية وسيلة كانت، مباشرة او غير مباشرة، وبشكل غير مشروع وبإرادته، يوفر أو يجمع الأموال بنية استخدامها أو هو يعلم أنها ستستخدم كلياً او جزئياً، للقيام:

... بأي عمل اخر يهدف الى التسبب في موت شخص مدني او اي شخص اخر، او اصابته بجروح بدنية جسيمة عندما يكون هذا الشخص غير مشترك في اعمال عدائية في حالة نشوب نزاع مسلح، عندما يكون غرض هذا العمل، بحكم طبيعته او في سياقه، موجها لترويع السكان، أو لإرغام حكومة أو منظمة دولية على القيام بأي عمل او الامتناع عن القيام به"[1].

والمقصـــود ب "الأموال" حســـب ما جاء في المادة 1 من ذات الاتفاقية انها " كل نوع من الاموال المادية وغير المادية المنقولة وغير المنقولة (العقارية) التي يتم الحصـــول عليها بأي وســـيلة كانت، والوثائق والصـــكوك القانونية أياً كان شـــكلها بما في ذلك الشـــكل الالكتروني والرقمي والتي تدخل على ملكية تلك

[1] الاتفاقية الدولية لقمع تمويل الإرهاب المعتمدة والمعروضة للتوقيع والتصديق بموجب قرار الجمعية العام رقم 54–109 المؤرخ في 9 كانون الأول/ديسمبر 1999.

الاموال او مصلحة فيها بما في ذلك، على سبيل المثال لا الحصر، الائتمانات المصرفية، وشيكات السفر، والشيكات المصرفية، والحوالات والأسهم والأوراق المالية والسندات والكمبيالات وخطابات الاعتماد".

وفي التشـــريع الفلســـطيني، جاءت النصـــوص مطابقة لحد ما مع تعريف الاتفاقية الدولية لجريمة تمويل الارهاب حيث نصت المادة (6) من قرار بقانون رقم 39 لسنة 2022 بشأن مكافحة غسل الاموال وتمويل الارهاب على انه:

1. يعد مرتكبًا لجريمة تمويل الإرهاب كل شـخص يقوم عمدًا بتقديم أو جمع الأموال من مصـدر مشـروع أو غير مشروع بأي وسيلة كانت مباشرة أو غير مباشرة، وبنية غير مشروعة لاستخدامها أو مع علمه بأنها ســوف تســتخدم كلياً أو جزئياً في ارتكاب عمل إرهابي أو من قبل شــخص إرهابي أو منظمة إرهابية.
2. يعد مرتكبًا لجريمة تمويل الإرهاب كل شـخص يقوم عمدًا بأي وسـيلة بصـورة مباشـرة أو غير مباشـرة بتقديم أو جمع الأموال من مصـدر مشـروع أو غير مشـروع بهدف سفر أفراد لدولة غير دولة إقامتهم أو جنسـيتهم بغرض ارتكاب أو تدبير أو المشـاركة أو الإعداد أو تسـهيل أعمال إرهابية أو توفير أو تلقي التدريب على الأعمال الإرهابية"[1].

كما شـــملت بالفقرة الثالثة من ذات المادة أي شـــخص يحاول او يســـاهم او يوجه اخرين لارتكاب جرائم ارهابية: " يعد أيضًا مرتكبًا لجريمة تمويل الإرهاب كل شخص:

1. يحاول ارتكاب جريمة تمويل الإرهاب
2. يشارك كطرف متواطئ في أي من جرائم تمويل الإرهاب أو محاولة ارتكابها.
3. ينظم جرائم إرهابية أو يوجه الآخرين لارتكابها أو لمحاولة ارتكابها.

[1] قرار بقانون رقم 39 لسنة 2022 بشأن مكافحة غسل الاموال وتمويل الارهاب.

4. يساهم في ارتكاب أو الشروع في ارتكاب جريمة تمويل إرهاب أو أكثر مع مجموعة من الأشخاص تعمل لغرض مشترك".

وكذلك اشار بالفقرة الخامسة الى "تنطبق جريمة تمويل الإرهاب حتى لو لم يقع العمل الإرهابي، أو لم تستخدم الأموال فعليًا لتنفيذه أو الشروع بتنفيذه، أو لم ترتبط الأموال بعمل إرهابي معين".

وبناءً على ذلك يمكن استنتاج ان جريمة تمويل الارهاب تقوم على ركنين اساسيين وهما الركن المادي والركن المعنوي، حيث يتمثل الركن المادي بالقيام بمجموعة من السلوكيات والتي تتمثل بجمع المال أو تقديمه بشكل كامل او جزئي في ارتكاب الاعمال الإرهابية او ان هذه الاموال سوف تستخدم من قبل شخص ارهابي او منظمة إرهابية.

اما فيما يتعلق بالركن المعنوي، أي القصد الجنائي والذي يتمثل بعلم الجاني واتجاه ارادته الى احداث السلوك والنتيجة، وهو ان الفعل الذي يقوم به يشكل جريمة يعاقب عليها القانون، فجريمة تمويل الارهاب من الجرائم العمدية التي تتطلب معرفة الجاني بالفعل الذي يقوم به اي معرفته بأن هذه الاموال سوف تستخدم لأغراض ارهابية وهو ما يعرف بالقصد الجنائي الخاص.

وفي الفضاء الالكتروني، تستخدم الجماعات الارهابية شبكة الانترنت في الحصول على تمويل لجرائمها مستغلة الفرص التي توفرها التقنية التكنولوجية من سهولة التواصل مع المستخدمين من مختلف بقاع العالم ونشر المعلومات وترويج الدعايات للجماعات الارهابية دون رقابة. ولعل من ابرز مصادر تمويل الارهاب هي التبرعات والتي من السهل الحصول عليها من خلال شبكة الانترنت، وقد يتم ذلك باستعطاف الافراد المستخدمين للشبكة بشتى الاساليب والوسائل وذلك لحملهم على دفع تبرعات مالية، او بإنشاء شركات وهمية تحت غطاء منظمات خيرية تهدف الى جمع الاموال والتبرعات.

او قد تم طوعاً حيث تطرق القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018 للتمويل عبر شبكة الانترنت، وذلك في الفقرة الثانية من المادة 18: "دون الاخلال بالأحكام الواردة في القرار بقانون بشـــأن مكافحة غسـل الأموال وتمويل الإرهاب النافذ، يعاقب كل من أنشـأ موقعاً أو تطبيقاً أو حسـاباً الكترونياً أو إحدى وسـائل تكنولوجيا المعلومات بقصـد... 2- القيام بارتكاب جريمة تمويل الإرهاب بالسـجن أو بغرامة لا تقل عن ثلاثة آلاف دينـار أردني، ولا تزيد على خمســـة آلاف دينـار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين."

فالركن المادي هنا يتمثل بإنشـاء صـفحة او موقعاً الكترونياً او حسـاباً او تطبيقاً الكترونياً، فبمجرد الانشـاء تتحقق الجريمة وتصـبح معاقب عليها، أي انه اعتبرها المشـرع من جرائم الخطر والتي لا يشـترط فيها وقوع التمويل فعلاً. كما انه اشترط فيها توافر القصد الجنائي.

الفرع الخامس: التجسس الالكتروني لصالح الجماعات الإرهابية

يعد التجســس من اخطر الجرائم التي يمكن ان تواجهها الدول ولاســيما بعد الانتشــار الواســع للشــبكة المعلوماتية في عصـــرنا الحالي، وذلك لما قد يترتب على هذه الجريمة من عواقب وخيمة على الأمن القومي، فالتجسـس فعل رافق نشـوء المجتمعات منذ القدم وتطور بتطورها، الامر الذي يضـعنا امام نوعين من التجسـس؛ التجسـس التقليدي والتجسـس الإلكتروني، فبالرغم من انهما يتفقان في الغرض والهدف، إلا انهما يختلفان في آلية ووسيلة الارتكاب.

تفادت معظم التشـريعات العربية ومنهم الاردني وضـع تعريف جامع ومانع للتجسـس، تاركين مهمة تعريفه للفقه. حيث عُرّف التجســس على انه " نقل معلومات قيمة ومهمة لصــالح دولة ما عن دولة اخرى، وذلك من خلال قيام تلك الدولة، بتوظيف الموارد البشـــرية، والأجهزة الالكترونية، والميزانيات المالية للقيام بهذه العملية، والتي يترتب عليها تســـهيل مهمتها، في القيام بأعمال عدائية ضـــد الدولة الأخرى التي نقلت معلوماتها" (مناصرة، 1991).

وأيضاً تم تعريف جريمة التجسس على انها: " تلك السلوكيات الإجرامية التي يأتيها الجاني تجاه بلده التي يحمل جنسيتها أو اتجاه البلد التي يقيم فيها، بهدف الحاق ضرر جسيم بأمنها القومي ووحدتها الإقليمية من خلال الاتصال والتواصل مع جهات أجنبية قد تكون معادية لبلده أو في حالة سلام معها وتزيدها بكل ما تحتاجه من معلومات أمنية عن بلده أو البلد التي يقيم فيها" (نابلسي، 2020).

اما التجسس الإلكتروني، كما ذكرنا سابقاً فهو يختلف عن التجسس التقليدي بالأداة المستخدمة وهي التقنية المعلوماتية التي توفر السرعة والسهولة في الحصول على المعلومات، وكذلك سهولة التخفي.

عرف الفقه التجسس الالكتروني على انه "الاطلاع على معلومات خاصة بالغير، محفوظة على جهاز الكتروني وليس مسموحاً لغير المخولين بالاطلاع عليها" (ابو غليون، 2009).

ومنهم من عرفه بأنه "سرقة المعلومات من الأفراد والمؤسسات العامة والخاصة والدول والمنظمات من اجل معرفه الحالة الاقتصادية والمالية والسياسية التي تعيشها الدولة ثم استغلالها من طرف المنظمات الإرهابية للقيام بعمليات إرهابية أو بيعها لدول معادية للدول المستهدفة ويستخدم في ذلك طرق تجسس مستعملة في ذلك أسلوب الاستيلاء على المعلومات الحساسة الهامة عن طريق إنفاق الرسائل الإلكترونية مجهولة المصدر ببرامج وتطبيقات إلكترونية من أجل فتح ثغرات إلكترونية في حاسوب الضحية أو الشبكة الكترونية المستعملة من طرفه" (عبد الحكيم ت.، 2021).

فنستنتج ان التجسس الالكتروني يعني قيام الجاني بالولوج الى نظام معلوماتي يحتوي على بيانات او معلومات غير متاحة للجمهور، تمس الامن الوطني أو السلامة العامة للدولة، والاعتداء عليها سواء من خلال حذفها أو تدميرها أو تغييرها أو إفشائها.

الفصل الثاني

دور اجهزة العدالة في مكافحة الاعتداءات الالكترونية على امن الدولة الداخلي

مما لا شك فيه ان أجهزة العدالة هي الوسيلة الأساسية في تحقيق الامن والاستقرار، وتحقيق الدفاع الاجتماعي، وتحقيق مصلحة المجتمع التي يتم الوصول اليها من خلال مكافحة الجريمة التي قد تمس شخص معين، ولكن بدورها فإنها تعبر عن خطر اكبر من ذلك وهو الخطر الذي يهدد امن المجتمع بأكمله.

لم يعد من الممكن مواجهة الاعتداءات الإلكترونية التي تهدد أمن الدولة الداخلي عبر الوسائل التقليدية فقط، خاصة في ظل تسارع وتيرة تطور الوسائل الرقمية المستخدمة في ارتكاب تلك الأفعال، وتعقيد الهياكل التقنية التي تُدار من خلالها. ومع انتقال التهديد من الفضاء الواقعي إلى الفضاء السيبراني، أصبحت أجهزة العدالة بمكوناتها المختلفة مطالبة بلعب دور مركزي ومتكامل في التصدي لهذه الاعتداءات، من خلال تطوير أدواتها القانونية والفنية، وتحديث إجراءاتها بما ينسجم مع طبيعة الجرائم التي تتجاوز الحدود الجغرافية والزمنية، وغالبًا ما تُرتكب من جهات يصعب الوصول إليها بالطرق التقليدية.

وتتضاعف أهمية هذه الحاجة في فلسطين نظراً لتعقيدات الوضع السياسي والأمني فيها، الى جانب محدودية القدرات التقنية ووجود فضاء رقمي مفتوح يمكّن اطرافاً داخلية وخارجية من التسلل الى البنية الاجتماعية والسياسية من خلال منصات التواصل الاجتماعي.

وتتوزع المسؤولية في هذا الإطار على عدد من المؤسسات المعنية، في مقدمتها الشرطة ممثلة بوحدة الجرائم الإلكترونية، التي تضطلع بمهمة تتبع الجرائم الرقمية والاعتداءات التي تستهدف الأمن العام والسيادة الوطنية. كما يبرز دور الجهاز الوقائي وغيره من الأجهزة الأمنية في رصد التحركات الرقمية ذات الطابع التحريضي أو الهدّام، وجمع الأدلة التقنية التي تُمكّن النيابة العامة من إقامة الدعوى الجنائية. ومع ذلك، لا تزال الإجراءات الجزائية المتبعة في فلسطين محكومة بقانون صدر في عام 2001، أي في مرحلة سابقة تمامًا لظهور التحديات السيبرانية المعاصرة، مما يطرح إشكاليات حقيقية حول مدى قدرة هذا الإطار

الإجرائي على استيعاب طبيعة الجريمة الإلكترونية، سواء من حيث الإثبات أو التبليغ أو إجراءات التفتيش والمصادرة (أبو العطا، 2016).

يهدف هذا الفصل إلى تسليط الضوء على كيفية تفاعل أجهزة العدالة الفلسطينية مع الاعتداءات الإلكترونية التي تمس أمن الدولة الداخلي، وتحليل مدى كفاية النصـوص القانونية والإجرائية في التعامل مع هذا النوع من الجرائم، إلى جانب عرض التجارب المقارنة في بلدان عربية مجاورة واجهت تحديات مشـابهة، وسـعت إلى تحديث أدواتها القانونية والأمنية في هذا المجال. كما يفتح الباب أمام مناقشـــة الآليات التي يمكن من خلالها مواءمة الإجراءات الجزائية الفلسطينية مع طبيعة التهديدات الرقمية، سواء من خلال تفعيل نصوص قائمة أو من خلال اقتراح آليات جديدة تنسـجم مع متطلبات التحقيق السـيبراني، وتضـمن فعالية الملاحقة القانونية، دون المساس بالضمانات الدستورية والحقوق الأساسية للمواطنين.

المبحث الاول: الدور القانوني والتنظيمي للأجهزة في فلسطين

قبل عام 2005، لم يكن هناك تشـــريع ينص على ماهية الأجهزة الأمنية العاملة في فلســـطين، حيث بلغ عددها آنذاك سبعة عشر جهازاً أمنياً، وبقيت هذه الأجهزة لا تستند الى هيكل تنظيمي واضـح لفترة طويلة من الزمن.

بعد تبني المجلس التشريعي الفلسطيني لقانون الخدمة في قوى الأمن رقم 8 لسنة 2005، تم تحديد الأجهزة الأمنية في ثلاث قوى رئيسة، فجاء في المادة 3 من القانون: "تتألف قوى الأمن من:

1. قوات الأمن الوطني وجيش التحرير الوطني الفلسطيني.
2. قوى الأمن الداخلي.
3. المخابرات العامة.

ان أجهزة العدالة بمختلف اشـكالها وصـورها تعرف على انها "عبارة عن مجموعة من المؤسـسـات التي اوجدتها الدولة لتامين النظام وحماية الافراد وممتلكاتهم حتى يسـعد الفرد في مجتمع يسـوده الامن والعدالة" (شحادة، 1999)، فهي الباعث على الشعور بالأمان والاستقرار، وهي الوسيلة الأساسية في تحقيق الرابطة

الإجرائية في الدعوى العمومية، وفي العمل الاجرائي، كما انها تمثل سـيادة الدولة على أراضـيها، وهذا ما نصت عليه المادة 6 من القانون الأساسي الفلسطيني[1]، وبالتالي فان أجهزة العدالة هي الوسيلة المخولة من قبل القانون بحفظ النظام العام مما قد يحدث من مشـاجرات ونزاعات وضـمان الراحة للناس في أماكنهم، ومراقبة تطبيق القوانين، وحفظ الجانب الأخلاقي في المجتمع، وتامين الحماية للأفراد جميعهم، وكذلك كشف ملابسات الجريمة من خلال العديد من الاجراءات التي تقوم بها والتي نص عليها قانون الإجراءات الجزائية والتي تبدا من لحظة وقوع الجريمة، وكيفية الحصول على الأدلة وجمعها.

ان أجهزة العدالة تقوم بالعديد من المهام التي من شـانها تحقيق نفس الغاية وهي تحقيق الامن والاسـتقرار في المجتمع، وتحقيق العدالة والدفاع الاجتماعي، الا ان هذه الاعمال تقوم على أساسيين وهما:

1. اعمال وقائية: وهي عبارة عن الاعمال التي تكون سـابقة على وقوع الجريمة، أي انها الاعمال التي يقوم بها رجال الامن ومنهم الشـرطة وغيرهم بحفظ الامن والاسـتقرار وحماية النظام العام للمجتمع بعناصـره المختلفة والمتمثلة بالأمن العام، الصـحة العامة، السـكينة العامة، والآداب والأخلاق في المجتمع.
2. اعمال قضـائية: وهي ممنوحة على سـبيل الحصـر لجزء من رجال السـلطة العامة وهي صـلاحية الضبط القضـائي، وهي مجموعة من السلطات القضـائية التي يمارسونها في حدود معينة، تهدف الى ملاحقة الجريمة واكتشـاف مرتكبيها وجمع الأدلة التي تلزم لمرحلة التحقيق في الدعوى (قرارية، 2017)، حيث ان من يتولى القيام بهذه المهام يطلق عليهم الضـابطة القضـائية، وهو الجهاز الذي يباشـر كافة الاجراءات التي تتخذها السـلطة القضـائية للتحري عن الجرائم بعد وقوعها والبحث عن مرتكبيها، تمهيدا للقبض عليهم، كما انها تقوم بجمع الادلة اللازمة للتحقيق كي يتنسـى لها امكانية توجيه التهمة له حتى يتم انزال العقاب بحقه (الإدريسي، 2018).

[1] تنص المادة 6 من القانون الأساسي المعدل على: مبدأ سيادة القانون أساس الحكم في فلسطين، وتخضع للقانون جميع السلطات والأجهزة والهيئات والمؤسسات والأشخاص.

تواجه الأجهزة الرسمية في فلسطين تحديات متصاعدة في مواكبة تطور أشكال الاعتداءات الإلكترونية، خاصة تلك التي تستهدف أمن الدولة الداخلي. فبينما تتوسع الفضاءات الرقمية وتزداد سهولة الوصول إلى الوسائل التقنية المستخدمة في تنفيذ هذه الاعتداءات، لا تزال البنية القانونية والتنظيمية التي تضبط عمل المؤسسات الرسمية في هذا السياق تعاني من فجوات واضحة، سواء من حيث الصلاحيات أو البنية التقنية أو الموارد البشرية. وتتركز جهود الدولة في هذا المجال ضمن عدد من الأجهزة الأمنية والشرطية التي تعمل على التعامل مع الجرائم الرقمية، لكن من منظور تقليدي لا يرقى غالباً إلى حجم التهديدات السيبرانية المعقدة التي باتت تطال البنية المؤسسية للدولة، وتؤثر على استقرارها السياسي والاجتماعي (المصري، 2011).

كما ويُلاحظ أن القوانين النافذة، وعلى رأسها قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001، لم تتضمن أي أحكام صريحة تتعلق بكيفية تنفيذ الإجراءات الجنائية في سياق الجرائم الإلكترونية، من حيث ضبط الأجهزة، مصادرة البيانات، أو إجراءات التفتيش الرقمي، ما يجعل بعض التدخلات عرضة للطعون القانونية، ويقلل من إمكانية استخدامها كأدلة قضائية. هذا القصور التشريعي لا ينعكس فقط على عمل الأجهزة الأمنية، بل يضع النيابة العامة والقضاء أمام صعوبات في تكييف الأفعال الرقمية ذات الطابع السيادي، ما يؤدي في بعض الحالات إلى إفلات الفاعلين من العقاب أو تصنيف الاعتداءات على أنها مجرد جرائم معلوماتية بسيطة[1].

---

[1] قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001م، رغم شموليته في تنظيم الإجراءات الجنائية التقليدية، لم يتضمن أحكامًا صريحة تتعلق بالجرائم الإلكترونية، مما يُحدث فراغًا تشريعيًا في هذا المجال. نصوص من القانون ذات الصلة:

المادة (1) : *تختص النيابة العامة دون غيرها بإقامة الدعوى الجزائية ومباشرتها، ولا تقام من غيرها إلا في الأحوال المبينة في القانون.*ديوان الجريدة الرسمية+1Palestine - Legal Databases+1

المادة (19) *يتولى أعضاء النيابة العامة مهام الضبط القضائي والإشراف على مأموري الضبط كل في دائرة اختصاصه.* ديوان الجريدة الرسمية+1mjr.ogb.gov.ps+1

المادة (39) *دخول المنازل وتفتيشها عمل من أعمال التحقيق لا يتم إلا بمذكرة من قبل النيابة العامة أو في حضورها، بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها، أو لوجود قرائن قوية على أنه يحوز أشياء تتعلق بالجريمة.*ديوان الجريدة الرسمية

المادة (50)*لا يجوز التفتيش إلا عن الأشياء الخاصة بالجريمة الجاري التحقيق بشأنها، ومع ذلك إذا ظهر عرضًا أثناء التفتيش وجود أشياء تعد حيازتها في حد ذاتها جرمية، أو تفيد بكشف الحقيقة في جريمة أخرى، جاز لمأمور الضبط القضائي ضبطها.*ديوان الجريدة الرسمية

المادة (51) *للنائب العام أو أحد مساعديه أن يضبط لدى مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص مرتكبها. كما يجوز له مراقبة المحادثات السلكية واللاسلكية، وإجراء تسجيلات لأحاديث في مكان خاص بناء على إذن من قاضي الصلح متى كان لذلك فائدة في إظهار الحقيقة في جناية أو جنحة يعاقب عليها بالحبس لمدة لا تقل عن سنة.*ديوان الجريدة الرسمية.

المصدر : قانون الإجراءات الجزائية رقم (3) لسنة 2001م – مقام+1Maqam+1Maqam

وبناء على ما سبق، فإن هذا المبحث يتناول الإطار القانوني والتنظيمي الذي يحكم عمل الأجهزة الرسمية الفلسطينية في التعامل مع الاعتداءات الإلكترونية التي تمس أمن الدولة الداخلي، بالأخص دور الشرطة (وحدة الجرائم الإلكترونية) في المطلب الأول، ومن ثم الجهاز الوقائي الفلسطيني في المطلب الثاني، باعتبارهما الجهتين الأكثر انخراطًا في هذا المجال.

كما يسعى إلى تحليل حدود الصلاحيات الممنوحة لهما، والمعيقات التي تواجه أداءهما، ومدى توافق تدخلاتهما مع القواعد القانونية الوطنية والمعايير المقارنة في الدول التي طورت بنيتها المؤسسية في المجال الرقمي.

المطلب الأول: دور الشرطة ووحدة الجرائم الإلكترونية

وحدة الجرائم الالكترونية هي عبارة عن الوحدة الرئيسية والتي تضم العديد من المهندسين المتمكنين وضباط موزعون على أفرع المباحث بحيث يقوم الضباط في أفرع المباحث باستقبال البلاغات والشكاوى وارسالها للوحدة الرئيسية ليتم العمل عليها ومتابعتها من خلال الفنيين والمهندسين للوصول للمشتبه به ويتم تزويد الافرع بتقرير خبرة فني من خلاله تتم ملاحقة المتهم ولحين تقديمه للقضاء ولهذه القضايا خصوصية عالية وسرية في العمل (مقابلة أجرتها الباحثة مع مدير المباحث في جهاز الشرطة الفلسطيني المقدم د. جهاد كميل في مدينة نابلس بتاريخ 2024/11/11).

في فلسطين تم إنشاء وحدة الجرائم الإلكترونية التابعة لإدارة المباحث العامة في الشرطة الفلسطينية عام 2013 وذلك بمبادرة من مدير عام الشرطة الفلسطينية بهدف الحد من الجرائم والمخاطر المترتبة على أمن المواطن وحماية خصوصيته وحريته وعدم ابتزازه او تهديده أو إسقاطه ويصبح فريسه لأصحاب الأجندات المعادية بالدولة والشعب والحفاظ على سلامة أمن المواطن والوطن (مقابلة أجرتها الباحثة مع ضابط في جهاز الشرطة الفلسطيني الأستاذ هيثم ياسين في مدينة نابلس بتاريخ 11/11/).

ان مركز الوحدة الرئيســي في رام الله، وفي كل مدينة يوجد قســم تابع لها وهي تتبع لإدارة المباحث العامة في مقر الشرطة الفلسطيني.

وســوف نتناول آلية عمل جهاز الشــرطة (وحدة الجرائم الالكترونية) في التعامل مع الجرائم الالكترونية، والتطرق لأبرز التحديات التي تواجهها في هذا السياق.

الفرع الأول: آلية تلقي البلاغات الالكترونية

تُعد آلية تلقي البلاغات الإلكترونية المدخل الأســاســي الذي تبدأ منه وحدة الجرائم الإلكترونية في التعامل مع القضـــايا التي تمس الأمن الرقمي الداخلي للدولة، وتكتســـب هذه الآلية أهمية بالغة لأنها تمثل نقطة التقاء المواطن أو الجهة المتضررة مع الجهاز الرسمي المسؤول عن الاستجابة للتهديدات الإلكترونية. وقد اعتمدت الوحدة في بداياتها على التبليغ المباشر من خلال الحضور الشخصي إلى مقار الشرطة، وهو ما كان يمثل عائقًا كبيرًا أمام كثير من الضحايا، خصوصًا في القضايا ذات الطابع السياسي أو الحساس، أو تلك التي ينطوي الإبلاغ عنها على مخاطر اجتماعية أو تهديدات أمنية.

ومع تطور الأداء المؤسسي، بدأت الوحدة تتبنى وسائل إلكترونية لتلقي البلاغات، مثل البريد الإلكتروني الرسمي أو النوافذ الإلكترونية التابعة لموقع الشرطة، حيث يمكن تقديم بلاغ الكتروني عبر بوابة الشرطة الفلسطينية الرسمية والتي تحتوي على نموذج خاص للإبلاغ عن الجرائم الالكترونية او من خلال وسائل التواصل الخاصة بها (الشرطة الفلسطينية)، او من خلال تطبيق خاص بالشرطة الفلسطينية والذي يشترط ان يتضمن سرداً للواقعة، مشفوعاً بما قد يتوفر من أدلة رقمية مثل الرسائل، الصور، الروابط أو أسماء حسابات، اضافةً الى بيانات المبلّغ الشخصية. ورغم توفر هذه الوسائل، فلا يزال الوعي المجتمعي بها محدوداً، وهذا بدوره يقلل من فرص اللجوء اليها خاصة في الحالات التي تحتاج الى تدخل فوري.

الفرع الثاني: التحقيقات الرقمية ووسائل الإثبات

يعرّف التحقيق بأنه مجموعة من الإجراءات التي تتبعها السلطات لاستظهار الحقيقة لجريمة معينة والتثبت من كافة أركانها وكشف جوانبها تمهيداً للمسؤولية وايقاع العقوبة على المتسبب. وتعرف كذلك علم متمم لقانون الجزاء وأصول المحاكمات الجزائية يرشد المحقق إلى السير في التحقيق من البداية إلى النهاية ويجمع الأدلة المثبتة لوقوعها، وكيفية ارتكابها والقبض على المتهم ومحاكمته (الأكاديمية العربية للعلوم المالية والمصرفية، 2016).

يُعتبر التحقيق الرقمي في القضايا ذات الطابع الإلكتروني من أكثر مراحل التعامل مع الجرائم تعقيداً، خاصة حين يتعلق الأمر باعتداءات تمس أمن الدولة الداخلي، نظراً لما تفرضه هذه التحقيقات من متطلبات فنية دقيقة وإجراءات قانونية توازن بين حماية الخصوصية وضمان فاعلية الملاحقة. في السياق الفلسطيني، لا تزال آليات التحقيق الرقمي تواجه إشكالات متعددة، سواء على صعيد غياب النصوص التي تنظم بشكل دقيق وسائل جمع الأدلة الرقمية، أو من حيث محدودية الإمكانيات التقنية والبشرية المتاحة لوحدة الجرائم الإلكترونية والجهات الأمنية ذات الصلة. فعلى عكس الجرائم التقليدية التي تعتمد على شهود أو تقارير مادية، فإن الاعتداءات الإلكترونية تُرتكب في فضاء افتراضي يصعب ضبطه، وغالباً ما يتم إخفاء أثرها، أو نشرها من جهات مجهولة تستخدم وسائل تمويه متقدمة، مثل الشبكات المشفّرة أو الحسابات الوهمية أو تقنيات التصفح المخفي (إبراهيم، أمن الجريمة الإلكترونية، 2008).

الفرع الثالث: التحديات التي تواجه الوحدة

ان التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في فلسطين وغيرها من دول العالم، فطبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية. ويقوم بالتحقيق في الجرائم الالكترونية نيابة متخصصة وفق إجراءات وقواعد إثبات خاصة، يساعدها في ذلك ضابطة قضائية متخصصة بالجرائم الالكترونية،

على عكس الجرائم التقليدية التي تختص بالتحقيق فيها النيابة العامة تساعدها الضابطة القضائية ذات الاختصاص العام وفقاً لقواعد التحقيق والإثبات التقليدية (مقابلة أجرتها الباحثة مع ضابط في جهاز الشرطة الفلسطيني الأستاذ هيثم ياسين في مدينة نابلس بتاريخ 2024/11/11).

ومن الصعوبات التي تواجه الجهاز في التعامل مع الجرائم الالكترونية عديده و أهمها عدم السيطرة على الانترنت داخل البلاد من قبل الجهاز حيث يوجد في بلادنا شبكات مزودة للإنترنت غير خاضعه للجهاز مثل الانترنت الاسرائيلي وعدم تعاون بعض الشركات وخصوصا التي تخضع للقوانين الأمريكية معنا مثل الفيسبوك و الاحتلال الاسرائيلي الذي يعيق في كثير من الاحيان وصول طواقمنا الى الأهداف التي يتم تتبعها و عدم توفر أجهزة و برامج هي ضرورية للعمل لدينا وذلك بسبب تكلفتها الباهظة و موجود جزء منها فقط لدى الوحدة الرئيسية التي تستقبل شكاوى من 11 محافظة عاملة ما يشكل ضغطا عاليا في العمل لديهم (مقابلة أجرتها الباحثة مع مدير المباحث في جهاز الشرطة الفلسطيني المقدم د. جهاد كميل في مدينة نابلس بتاريخ 2024/11/11).

المطلب الثاني: دور الجهاز الوقائي الفلسطيني في الاعتداءات الالكترونية على أمن الدولة الداخلي

نشأ جهاز الامن الوقائي كجهاز يمكنه الحفاظ على الأمن الداخلي للسكان الفلسطينيين منذ تولي السلطة الوطنية الفلسطينية للحكم في الأراضي الفلسطينية في العام 1994، حيث بقي هذا الجهاز يمارس أعماله بشكل مستقل دون أن يكون هناك قانون ينظم عمل الجهاز حتى عام 2002 عندما تم الحاق جهاز الأمن الوقائي بوزارة الداخلية بموجب مرسوم رئاسي، وأصبح عمله أكثر وضوحاً في عام 2005مع صدور قانون الخدمة في قوى الأمن الفلسطيني.

وفي عام 2007 أصدر الرئيس الفلسطيني قراراً بقانون، بشأن الأمن الوقائي رقم (11) لسنة 2007، حيث نص على اعتبار جهاز الوقائي إدارة عامة أمنية نظامية، ضمن قوى الأمن الداخلي، التي تتبع وزارة الداخلية، وتعمل في مجال الأمن، وتضمّن مهام الجهاز ومنحه صفة الضبط القضائي، واعتبر مراكز

التوقيف التابعة له قانونية، وحصر وظيفته في حماية الأمن الداخلي الفلسطيني ومتابعة كافة القضايا التي قد تمس او تهدد الامن الداخلي.

تنص المادة 6 من القرار بقانون بشـــأن الامن الوقائي على مهام الجهاز: "بما لا يتعارض مع القوانين السارية تعتبر الإدارة العامة للأمن الوقائي الجهة المكلفة بما يلي:

1. العمل على حماية الأمن الداخلي الفلسطيني.
2. متابعة الجرائم التي تهدد الأمن الداخلي للســـلطة الوطنية و/ أو الواقعة عليه، والعمل على منع وقوعها.
3. الكشف عن الجرائم التي تستهدف الإدارات الحكومية والهيئات والمؤسسات العامة والعاملين فيها".

حيث يقوم جهاز الامن الوقائي بمتابعة الصفحات المشبوهة والمدسوسة والتي تعمل على اثارة الفوضى والفتن واثارة النعرات وبالتالي القاء القبض على اصحاب تلك الصفحات والناشرين فيها وتقديمهم للعدالة، حيث تبدأ بمتابعة تلك الصفحات والحسابات والمواقع والاحتفاظ بما ينشر ويكتب كدليل قاطع تمهيدا لتقديم المجرم للقضاء، ومن الاجراءات المتبعة استدعاء المتهم واستجوابه ومراجعته بما ينشر ويكتب من قبل النيابة العامة واحينا تتم مداهمة وتفتيش بيت او سكن المتهم بعد الحصول على امر من النيابة.

ومن الإجراءات التي يتخذها الجهاز للحد من هذه الجرائم ومنع وقوعها (مقابلة مع مدير قسم امن الجهاز الوقائي بالاشتراك مع مدير قسم تكنولوجيا المعلومات في مدينة نابلس بتاريخ 2025/2/20):

1. التوعية الاجتماعية والتحذير من التعاطي مع تلك المواقع من خلال ندوات تعقدها دائرة العلاقات العامة والسلم الاهلي بالشركة مع الأجهزة الاخرى والتوجيه السياسي تستهدف طلبة المدارس والجامعة كونهم الاكثر عرضه للاستهداف.
2. تعطيل تلك المواقع والحسابات واغلاقها.

فنستنتج ان الجهاز الوقائي في فلسطين يعمل ضمن منظومة الأمن الداخلي التي تهدف إلى حماية الدولة من التهديدات التي قد تؤثر على استقرارها السياسي والمجتمعي. ورغم أن هذا الجهاز تاريخياً كان يُعنى بمهام مرتبطة بالمخاطر الأمنية التقليدية، إلا أن التحولات الرقمية فرضت واقعًا جديدًا، ألزمه بتوسيع نطاق عمله ليشمل الجرائم والاعتداءات الإلكترونية، خصوصاً تلك التي تمس النظام العام والسيادة الوطنية. مع ذلك، لا توجد في فلسطين نصوص قانونية صريحة تُحدّد طبيعة الصلاحيات الرقمية لهذا الجهاز، ما يجعل تدخله في بعض الحالات غير محاط بإطار قانوني واضح، ويُعرّض إجراءاته للطعن من جهة، ويقلل من التنسيق المؤسساتي من جهة أخرى.

وفي ظل غياب هذا التنظيم القانوني، يعتمد الجهاز في عمله الإلكتروني على اجتهاداته الأمنية، التي قد تختلف في تقدير الخطورة من حالة لأخرى. وتتمثل صلاحياته الفعلية في الرصد الرقمي الاستباقي، وجمع المعلومات من خلال تحليل المحتوى المنشور عبر الإنترنت، أو مراقبة التفاعلات الرقمية ذات الطابع التحريضي أو التحريكي. لكن هذه الصلاحيات تظل محدودة في قدرتها على التحرك القضائي، إذ لا يمتلك الجهاز سلطة الضبط أو التوقيف، ما يستوجب التنسيق مع جهات أخرى مثل الشرطة أو النيابة.

الفرع الأول: الرقابة على الانترنت ضمن القانون

تُثار دائمًا في السياقات التي تتعامل مع الأمن الرقمي إشكالية التوازن بين متطلبات الرقابة والضبط، وحقوق الأفراد في استخدام الإنترنت وحرية التعبير. في فلسطين، يقوم الجهاز الوقائي بدور رقابي على محتوى الإنترنت، لا من منطلق قمعي أو استبدادي، وإنما من منطلق أمني يهدف إلى منع الانفجار الداخلي أو ردع التنسيق مع جهات خارجية تستغل الفضاء الرقمي لأغراض تخريبية. غير أن هذه الرقابة لا تستند إلى نص قانوني صريح يحدد أدواتها وحدودها، وإنما تتم وفق مذكرات أو تعليمات إدارية داخلية، مما يفتح الباب لانتقادات حقوقية تتعلق بإمكانية التعدي على الخصوصية أو الحريات الرقمية.

كما أن عدم وجود إطار قانوني واضـــح يُعرّف مفهوم "التحريض الرقمي" أو "الاعتداء على الســـيادة عبر الإنترنت" يجعل من أي رقابة إلكترونية عملًا غير مؤطر قانونيًا، وقد يؤدي إلى توتر العلاقة بين الجهاز والمجتمع المدني. ولكي تكون الرقابة على الإنترنت مشروعة وفعالة، لا بد من تضمينها ضمن نصوص قانونية واضحة، تُحدد طبيعة المحتوى الخطر، وتربط الرقابة بالحصول على إذن قضائي في الحالات التي تتطلب تدخلًا مباشرًا.

الفرع الثاني: كشف الشبكات الداخلية والخارجية

من أخطر ما يواجه الأمن الداخلي اليوم هو وجود شـبكات رقمية منظمة تنشـط من الداخل بالتنسـيق مع جهات خارجية، وتعمل على تنفيذ أجندات ســياســية أو أمنية معادية من خلال محتوى رقمي منسّــق أو حملات منظمة على وسـائل التواصـل. الجهاز الوقائي مكلف برصـد هذه الشـبكات وتحليل بنيتها واختراق حلقاتها لكشف مصادر تمويلها، وأهدافها الحقيقية، والجهات التي تُسيّرها. غير أن هذا العمل يتطلب أدوات تحليل متقدمة ومهارات اســتخبارية دقيقة، لا تزال محدودة الإمكانيات في البيئة الفلســطينية. ومع غياب أدوات الذكاء الاصـطناعي، والبرمجيات المعتمدة على التعلم الآلي، لا يمكن للوحدة أن تواكب حجم التدفق المعلوماتي على المنصات الرقمية، ولا أن تحدد أنماط التكرار أو التوجيه التي تشير إلى وجود تنسيق غير عفوي بين الداخل والخارج (العادلي، 2006).

كما أن العمل الاســتخباري في المجال الرقمي يتطلب تعاونًا دوليًا فعّالًا مع المنصــات العالمية ومزودي الخدمات الإلكترونية، وهو تعاون غالبًا ما لا يتوفر نظرًا لمحدودية الاعتراف القانوني أو ضــعف النفاذ الدولي للجهات الفلســطينية. لذا، فإن بناء قدرات تحليل الشــبكات الرقمية المنظمة يجب أن يكون أولوية وطنية، من خلال دعم الجهاز الوقائي بالأدوات الفنية والتشــريعية والبشــرية التي تُمكّنه من كشــف هذه الأنشطة، والتصدي لها في بدايتها، قبل أن تتحول إلى تهديد فعلي للاستقرار الداخلي.

الفرع الثالث: التحديات القانونية واللوجستية

يواجه الجهاز العديد من الصـــعوبات والتعقيدات في التعامل مع الجرائم الالكترونية وبالأخص الاعتداءات الالكترونية على الامن الداخلي والتي من أهمها (مقابلة أجرتها الباحثة مع مدير قســم امن الجهاز الوقائي بالاشتراك مع مدير قسم تكنولوجيا المعلومات في مدينة نابلس بتاريخ 2025/2/20):

1. ان تلك الصفحات والحسابات وهمية وتدار من خارج حدود الوطن.
2. الشرائح الإسرائيلية تكون عائق للتعرف على المجرم.
3. نقص جزئي في الكادر المهني المختص.

فالجهاز الوقائي في فلسطين يواجه تحديات مزدوجة، تتعلق من جهة بغياب البيئة القانونية المناسبة لعمله في المجال الرقمي، ومن جهة أخرى بضـــعف الإمكانيات اللوجســـتية التي تحول دون تطوير قدراته الاسـتخبارية والتقنية. من الناحية القانونية، لا يوجد حتى الآن قانون صـريح يُنظم عمل الجهاز الوقائي أو يُحدّد مهامه في المجال الإلكتروني، ما يضعه في موقع حساس بين الضرورات الأمنية والقيود الدستورية. فالممارسات التي يضطر إليها الجهاز، مثل الرصد الرقمي، أو التحليل الاستباقي للبيانات، أو حتى مراقبة بعض الحســابات المشــتبه بها، قد تُفســر من قبل بعض الجهات على أنها تجاوز للســلطة أو تدخل في الحريات، رغم أن الواقع يفرضها كضرورة لحماية السلم الأهلي ومنع الاختراق السياسي.

أما من الناحية اللوجستية، فإن الجهاز يعاني من نقص حاد في البنية التكنولوجية، سواء على صعيد المعدات أو البرمجيات، فضلًا عن غياب فرق تحليل متخصصة في الذكاء الاصطناعي أو الهندسة الاجتماعية أو تحليل البيانات الضخمة، وهي جميعها أدوات أصبحت ضرورية في بيئة رقمية مشبعة بالمخاطر.

هذا النقص القانوني واللوجسـتي يُضـعف من قدرة الجهاز على مواكبة التهديدات المتسـارعة، ويجعل عمله قائمًا على ردود الأفعال لا على خطط استباقية، الأمر الذي يستدعي إعادة نظر شاملة في تمويل الجهاز، وتأطيره قانونيًا، ودمجه ضمن استراتيجية وطنية متكاملة للأمن السيبراني (الهاجري).

المبحث الثاني: تحليل الإجراءات المتبعة في المكافحة

إن الاعتداءات الإلكترونية التي تستهدف أمن الدولة الداخلي لا يمكن مواجهتها بمجرد أدوات أمنية أو تقنية، بل تتطلب منظومة إجرائية متكاملة تبدأ منذ لحظة رصد الفعل وحتى لحظة المحاسبة القضائية. ويُعد النظام الإجرائي الجنائي، ممثلًا في الإجراءات القانونية المتبعة في التحقيق والملاحقة والمحاكمة، العمود الفقري الذي تستند إليه الدولة في مواجهة هذه التحديات (احمد، 2007). غير أن هذه الإجراءات، كما هي مطبقة في فلسطين، لا تزال مستندة إلى قانون الإجراءات الجزائية الصادر سنة 2001، وهو قانون صيغ في حقبة لم تكن فيها الجرائم الإلكترونية قد تشكلت بوصفها تهديدًا مستقلًا، ولم يكن فيها الفضاء الرقمي قد دخل بعد في صميم التفاعلات السياسية والاجتماعية والاقتصادية. هذا الانفصال الزمني بين واقع الجريمة وحدود النصوص الإجرائية التقليدية يخلق حالة من عدم المواءمة، تضع مؤسسات إنفاذ القانون أمام معضلة حقيقية، تتمثل في محاولة استخدام أدوات قديمة لمواجهة تهديدات حديثة تتسم بالسرعة والتعقيد والتداخل العابر للحدود (السنباطي، 19–20 يونيو 2007).

ومع تنامي الاعتداءات الرقمية التي تمس الأمن الداخلي، أصبح من الضروري دراسة مدى كفاية الإجراءات التقليدية القائمة، وبحث إمكانية توظيفها في نطاق الجرائم الالكترونية، دون أن تفقد فعاليتها أو مصداقيتها القانونية. كما تبرز الحاجة إلى البحث في الإجراءات المستحدثة التي بدأت بعض الأنظمة القانونية في اعتمادها لملاحقة هذا النوع من الاعتداءات، سواء على مستوى التفتيش الرقمي، أو التتبع الإلكتروني واعتراض البيانات، وتحليل البيانات الرقمية.

المطلب الأول: إجراءات مستحدثة لمكافحة الاعتداءات الإلكترونية في التشريع الفلسطيني

مع تصاعد وتيرة الاعتداءات الإلكترونية واتساع نطاق تأثيرها على بنية الدولة واستقرارها الداخلي، بات من الضروري عدم الاكتفاء بالإجراءات التقليدية في مواجهتها، خصوصاً وأن هذه الاعتداءات غالباً ما تتخذ أشكالاً معقدة وتُنفذ من جهات مجهولة أو عابرة للحدود الجغرافية والسياسية.

في السـياق الفلسـطيني، ما زالت الإجراءات المسـتحدثة في مراحلها الأولية، إن لم تكن غائبة في بعض الجوانب. فباسـتثناء بعض الاجتهادات الأمنية المحدودة، لا يوجد حتى اللحظة إطار تشـريعي أو تنظيمي شـامل يقرّ إجراءات مخصـصـة للتعامل مع الاعتداءات الالكترونية التي تهدد امن الدولة الداخلي، وهذا الوضـع يُضـعف من قدرة الدولة على المواجهة الاستباقية، ويجعل الأجهزة الأمنية والقضـائية تعمل ضـمن هامش ضيق، مما يترك ثغرات مكشوفة في جسد الأمن الداخلي. ومن هنا، تأتي أهمية هذا المطلب، الذي يسعى إلى تحليل النصوص المتعلقة بالإجراءات المستحدثة لدراسة مدى قدرتها على مواجهة هذا النوع من الاعتداءات.

الفرع الأول: التفتيش الإلكتروني

يُعد التفتيش من أبرز الوسائل التي تستخدمها الجهات الأمنية في جمع الأدلة، وقد تطور في البيئة الرقمية إلى ما يُعرف بالتفتيش الإلكتروني، الذي يقوم على فحص الأجهزة والمحتوى الرقمي والحسابات الافتراضية بحثًا عن أدلة على وجود نشاط إجرامي يمس الأمن الداخلي.

عرّفت محكمة النقض المصـــرية التفتيش بأنه "التفتيش كما هو معروف في القانون هو ذلك الإجراء الذي رخص به الشارع التعرض لحرمة الشخص بسبب جريمة وقعت او ترجح وقوعها منه ذلك تغليباً للمصلحة العامة على مصالح الأفراد الخاصة واحتمال الوصول الى دليل مادي يكشف الحقيقة." (مصطفى، 2010)

ويعرّف التفتيش في الجرائم الالكترونية على انه عملية بحث وتنقيب في وعاء السـر بقصـد ضـبط ما يفيد في كشـــف الحقيقة، فالهدف من إجراء التفتيش في الجرائم الالكترونية هو الوصـــول إلى ادلة مادية أو معنوية تفيد في كشف الحقيقة وكشف المتهم ونسب الجريمة إليه (العبيدي، 2013).

لكن هذا النوع من التفتيش يطرح إشـكالات قانونية حقيقية في ظل غياب نصـوص صـريحة في القانون الفلسـطيني تنظم شـروطه، وحدوده، وضـماناته. فبينما كان التفتيش التقليدي يتم على مكان مادي وتحت رقابة واضـحة من السلطة القضـائية، فإن التفتيش الإلكتروني يستهدف معطيات افتراضـية لا يمكن تقييدها

بمكان، ولا تُحاط بنفس الضمانات، ما يفتح الباب لاحتمالات المساس بالخصوصية أو إساءة استعمال السلطة.

لم يتطرق القرار بقانون رقم 10 لسنة 2018 الى تعريف التفتيش الالكتروني، وانما اقتصر على بيان آلية التفتيش الالكتروني والتي تتم بشكل أساسي عن طريق النيابة العامة او بانتدابها المؤهلين فنياً وقانونياً من مأموري الضبط القضائي للقيام بتفتيش اشخاص وأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، فإذا أسفر هذا التفتيش عن ضبط أجهزة او أدوات او وسائل ذات صلة بالجريمة، يتعين الحصول على اذن آخر للتفتيش من وكيل النيابة وهو ما يسمى بالنفاذ المباشر وذلك للولوج الى المكنونات المعنوية للأجهزة المضبوطة[1]. فالحصول على اذن آخر للتفتيش يشكل ضمانة أساسية لحماية الحريات العامة وخصوصية الافراد بما ينسجم مع احكام القانون الأساسي الفلسطيني، حيث يعد هذا النوع من التفتيش حساساً نظراً لما قد يحتويه الجهاز الالكتروني من بيانات قد تمس الحياة الخاصة للأفراد.

فنستنتج ان التفتيش في الجرائم الالكترونية ينقسم الى نوعين، الأول يعتبر تفتيش واقعي ويكون الهدف من وراءه ضبط ماديات الجريمة أي الأدوات المستخدمة في الجريمة كالحاسوب او أي جهاز الكتروني، والنوع الثاني تفتيش معنوي، أي البحث بمكنونات هذا الجهاز الداخلية وتحليلها لاستنباط الدليل القاطع، وذلك بعد الحصول على اذن بالتفتيش.

[1] نص المادة 52 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات: "1. للنيابة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة. 2. يجب ان يكون أمر التفتيش مسبباً ومحدداً ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الاجراء قائمة. 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة او أدوات او وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على النيابة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل النيابة ان يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الالكترونية."

وفيما يتعلق بشروط اذن او امر التفتيش، حيث جاء في الفقرة الثانية من المادة 52 من القرار بقانون بشأن الجرائم الالكترونية وجرائم الاتصـالات انه "2. يجب ان يكون امر التفتيش مسـبباً ومحدداً، ويجوز تجديده اكثر من مرة، ما دامت مبررات هذا الإجراء قائمة".

وترى الباحثة ان إبقاء مدة سـريان تنفيذ الاذن مفتوحة وإمكانية تجديدها لأكثر من مرة قد يشـكّل مسـاسـاً بخصـوصـية الافراد والحريات العامة، فينبغي ان تكون هذه المدة محصـورة بنطاق زمني محدد بما يراعي خصوصية الافراد وعدم انتهاك الحياة الخاصة.

كما أوجب المشرع الفلسطيني الجهات المختصـة بالتفتيش الالكتروني تدوين محضراً بكافة الإجراءات التي اتخذوها في سبيل ذلك، فجاء في المادة 54 من القرار بقانون بشـأن الجرائم الالكترونية وجرائم الاتصـالات في الفقرة الأولى منها "... وعلى من قام بالتفتيش أو المراقبة أو التسـجيل أن ينظم محضـراً بذلك يقدمه للنيابة العامة."، وبالرجوع للقواعد العامة في التفتيش، يجب تدوين كافة الإجراءات التي قاموا فيها، وما تم ضبطه من أشياء ذات صلة بالجريمة الجاري التحقيق بشأنها، وكذلك تدوين الملاحظات التي يبديها المتهم أو الشـهود الحاضـرين وفيما اذا وقع أي شـيء قد يعيق عملية التفتيش، فمثلاً في حالة تفتيش الأجهزة الالكترونية التي تتطلب كلمة مرور من صـاحبها ويمتنع عن فتحه او إعطائها لمأموري الضـبط القائمين بالتفتيش، وكذلك تدوين الحالة التي كانت عليها الأجهزة عندما تم ضبطها.

وفيما يتعلق بتفتيش الوسـائل التكنولوجية الخاصـة بأنثى، فلم يتطرق المشـرع الفلسـطيني في القرار بقانون بشـأن الجرائم الالكترونية لذلك، وترى الباحثة انه من الاصـوب الرجوع للقواعد العامة الواردة في قانون الإجراءات الجزائية الفلسـطيني، والتي تنص على انه لا يتم تفتيش الانثى إلا من قبل انثى[1]. وعليه اذا كانت الوسائل تعود لأنثى فيجب ان يتم التفتيش بواسطة انثى منتدبة لذلك لحماية خصوصيتها.

[1] المادة 47 من قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001: " اذا كان الشخص المراد تفتيشه انثى، فلا يجوز تفتيشها الا بواسطة انثى ينتدبها لذلك القائم بالتفتيش."

الفرع الثاني: الحصول على المعلومات من مزودي الخدمة

جاء في القرار بقانون رقم 10 لسـنة 2018 مجموعة من الالتزامات التي تقع على عاتق مزودي الخدمات في فلسطين، والتي تتمثل بتزويد الجهات المختصـة بأي معلومات خاصـة بالمشترك ذات الصـلة بموضـوع الجريمة والتي قد تساعد في كشف الحقيقة وذلك بناءً على طلب النيابة او المحكمة المختصة[1].

حيث عرّف القانون مزود الخدمة " أي شـخص يقدم لمسـتخدمي الخدمة الخاصـة به القدرة على الاتصـال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب نيابة عن أي خدمة إلكترونية أو مستخدمي هذه الخدمة[2]".

هذا يدفعنا للتساؤل عن طبيعة هذه المعلومات ونوعها، وكيف يمكنها ان تساعد في كشف الحقيقة.

لقد عرّف المشـرع الفلسـطيني معلومات المشـترك بأنها " المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة[3]".

فنوع الخدمة المسـتخدمة والشـروط الفنية والتي تكون عبارة عن بيانات مرتبطة بالأجهزة والشـبكة وآلية لاتصال، كعنوان ال IP، ورقم ال IMEI، وعنوان ال (MAC (Media Access Control Address، والبروتوكولات المستخدمة، وكذلك اعدادات الشبكة وسرعة الاتصال.

حيث يعد كل من عنوان بروتوكول الإنترنت (IP Address)، وعنوان التحكم بالوصـول الى الوسـائط (MAC (Media Access Control Address، من العناصـر الجوهرية التي تدخل ضـمن ما يُعرف

[1] الفقرة 1 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[2] المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

[3] المادة 1 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

بالشروط الفنية لمعلومات المشترك، والحصول عليها من مزودي الخدمة يساعد في كشف الحقيقة وذلك عن طريق عنوان ال IP حيث يساهم في تتبع مصدر الاتصال وربطه بالمشترك من خلال بيانات مزود الخدمة، وعنوان MAC لإثبات هوية الجهاز المادي، بمعنى تحديد بالضبط أي جهاز استُخدم في الجريمة. وهذا ما يوفر للجهات المختصة أدلة تساعد على الربط بين النشاط الالكتروني والفاعل أو الجهاز المستخدم.

فبالتالي وبحسب القرار بقانون، على مزودي الخدمة تزويد الجهات المختصة بهذه المعلومات بناءً على طلب النيابة او المحكمة المختصة. وكذلك وبناء على الأوامر الصادرة الى مزود الخدمة من الجهات القضائية حجب رابط أو محتوى أو تطبيق على الشبكة الالكترونية[1]، مع مراعاة احكام المادة 59 من ذات القانون والتي سنتناولها بالتفصيل في الفرع الرابع.

كما يقع على عاتق مزود الخدمة الاحتفاظ بمعلومات المشترك مدة لا تقل عن ثلاث سنوات لغايات تزويد الجهات المختصة فيها عند الطلب لمساعدتها في كشف الحقيقة[2]. وبناء على قرار قاضي المحكمة المختصة يتعاون مزود الخدمة مع الجهات المختصة في جمع وتسجيل المعلومات أو البيانات الالكترونية والاحتفاظ المؤقت بها[3].

الفرع الثالث: الاعتراض الالكتروني من قبل الجهات المختصة

لم يتطرق المشرع الفلسطيني الى تعريف ما المقصود بالاعتراض الفوري لمحتوى الاتصالات سواء السلكية أو اللاسلكية او أية وسيلة اتصال مكتوبة، الا انه نظّم في القرار بقانون رقم 10 لسنة 2018 إجراءات تنفيذ هذا الاعتراض.

[1] الفقرة 2 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.
[2] الفقرة 3 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.
[3] الفقرة 4 من المادة 51 من القرار بقانون رقم 10 لسنة 2018 وتعديلاته بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

عرّف الفقهاء الاعتراض بأنه "التتبع السري والمتواصل لمراسلات المشتبه فيه قبل واثناء وبعد ارتكابه للجريمة" (عمارة، 2010)، كما يعرّف على انه "اجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانوناً بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث" (محلق، 2015).

ويتم الاعتراض باستخدام وسائل فنية تتعلق بالتنصت والتحكم أو مراقبة محتوى الاتصالات، كذلك يمكن أن تشمل وسائل الاعتراض على تسجيل البيانات (شرف الدين، 2017)، وهذا ما يميِّزه عن التسجيل الصوتي الذي يجريه رجال الضبطية القضائية أثناء المراقبة الهاتفية، فهذا الأخير يستعمل في تحليل المكالمات الهاتفية المسجلة، وإخضاع عينات منها للتحليل، لتحديد نبرات صوت المتحدث (المشتبه فيه) الذي أُخضع هاتفه للمراقبة، إضافة إلى إمكانية تحديد المكان الذي اتصل منه، والاطلاع على فهرس المكالمات الهاتفية التي أجراها المشتبه فيه بتبيان الأرقام المتصلة والمتصل بها (غلاب و كيسي، 2019).

ويفرق الفقه بين مصطلح اعتراض المكالمات الهاتفية وبين مصطلح وضع الخط الهاتفي تحت المراقبة، فبينما يكون الأول دون رضا المعني فيكون الثاني بطلب أو برضا صاحب الشأن ويخضع لتقدير الهيئة القضائية بعد تسخير مصالح البريد والمواصلات لذلك (خلفي، 2010). فإجراء المراقبة الهاتفية لا يخضع لنفس الشروط التي تحكم أسلوب الاعتراض، بل يكفي أن تكون بطلب أو رضا من الشخص صاحب الشأن، حيث يحق للمتضرر او ضحية الجريمة أن يتقدم بطلب من اجل اخضاع هاتفه للمراقبة، على عكس الاعتراض.

نصت المادة 56 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات على انه:

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو احد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والافعال الموجبة له، ومدته.

2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشـهر من بداية تاريخ الشـروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.

3. يتعين على الجهة المكلفة بتنفيذ اذن الاعتراض إعلام النيابة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها".

فالاعتراض يمكن ان يكون في مرحلة ســـابقة لوقوع الجريمة وأثناءها وبعدها وذلك بإذن من قبل المحكمة المختصــة بناءً على طلب مقدم لها من النائب العام أو احد مسـاعديه. كما وحدد المشـرع الفلسـطيني مدة زمنية لا تزيد على ثلاثة أشهر لإتمام عملية الاعتراض، مع إمكانية تمديد لمرة واحد فقط،

وترى الباحثة انه كان الاجدر بالمشـــرع الفلســـطيني تحديد الجرائم التي يجب أن يُتخذ بشـــأنها إجراءات الاعتراض، كالجرائم الأمنية أو الاعتداءات التي تقع الكترونياً على الامن الداخلي للدولة نظراً لخطورتها ولطابعها الاجرامي المعقد، فبالرغم من أهمية اجراء الاعتراض الفوري لمحتوى الاتصـالات من قبل الجهات المختصـة في حماية المجتمع والحفاظ على استقراره واستباب الأمن فيه، الا انه قد يشكّل مساساً بحريات الافراد.

الفرع الرابع: حجب المواقع الالكترونية

نصت المادة 59 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات على انه:

1. لجهات التحري والضـبط المختصـة، اذا ما رصـدت قيام مواقع الكترونية مسـتضـافة داخل الدولة او خارجها، بوضع أي عبارات او ارقام او صور او أفلام او أي مواد دعائية أو غيرها، من شأنها تهديد الأمن القومي او النظام العام او الآداب العامة، أن تعرض محضـــراً بذلك على النائب العام أو احد مساعديه، وتطلب الاذن بحجب الموقع او المواقع الالكترونية او حجب بعض روابطها من العرض.

2. يقدم النائب العام او احد مسـاعديه طلب الاذن لمحكمة الصـلح خلال 24 سـاعة، مشـفوعاً بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم عرضه عليها إما بالقبول أو الرفض، على ألا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة.

تناولت هذه المادة بدايةً اختصاصات مأموري الضبط القضائي، حيث تعتبر إجراءات المراقبة والرصد من إجراءات التحري والاستدلال والتي هي اختصاص اصيل لمأموري الضابطة القضائية والتي تتم تحت اشراف النيابة العامة، وهي تسبق عملية الحجب، فبعد تدوين محضر بما تم رصده من مواقع الكترونية او اي روابط تمس بالنظام العام او تشكل تهديداً على امن الدولة الداخلي، يُقدم مأموري الضبط طلب للنائب العام او احد مساعديه لحجب هذه المواقع، والذين بدورهم يقدموا الطلب لمحكمة الصلح للنظر في شأنه وإصدار قرارها في ذات يوم عرضه عليها.

ومن التطبيقات القضائية لنص المادة 39 من القرار بقانون، أصدرت محكمة صلح رام الله قراراً بتاريخ 2025/1/5 في الطلب المقدم من النائب العام رقم (2025/01) يقضي بحجب مواقع وروابط الكترونية لمدة أربعة أشهر. وتنفيذاً للقرار حذفت الشركات المزوّدة لخدمة الانترنت في الضفة الغربية المواقع الالكترونية التي شملها القرار.

وكذلك القرار الصادر عن محكمة صلح رام الله في الطلب رقم 2019/12 بتاريخ 2019/10/17 والذي يقضي بحجب عدد من المواقع الالكترونية، حيث ورد في قرار المحكمة أن تلك المواقع تقوم بنشر ووضع عبارات وصور ومقالات عبر الشبكة العنكبوتية من شأنها تهديد الأمن القومي والسلم الأهلي والإخلال بالنظام العام والآداب العامة وإثارة الرآي العام الفلسطيني.

المطلب الثاني: إجراءات حديثة لمكافحة الاعتداءات الإلكترونية لم يتناولها المشرع الفلسطيني

تعتبر شبكات التواصل الاجتماعي اليوم احدى اقوى الأدوات التي تُستعمل في تنفيذ الاعتداءات الإلكترونية على الأمن الداخلي للدول، نظراً لما توفره من مساحة مفتوحة للنشر والتفاعل مع جمهور واسع. فلم تعد هذه المنصات مجرد وسيلة للتواصل بين الأفراد، بل تحولت إلى ساحة افتراضية تشهد صراعات سياسية، واختراقات للبيانات الحكومية، وتجنيد لصالح جماعات إرهابية وغيرها من السلوكيات التي تؤثر بشكل مباشر على الاستقرار والامن الداخلي ووحدة المجتمع.

ويكمن التحدي الأكبر في قدرة هذه الاعتداءات على التسلل إلى الوعي الجماعي بهدوء، فتزداد خطورة هذه المسألة في المجتمع الفلسطيني بسبب هشاشة الوضع السياسي وتعدد الجهات الفاعلة في المشهد الرقمي، فضلًا عن محدودية الإمكانيات التقنية والقانونية في التصدي لهذه الظاهرة.

وفي ظل هذا التصـــاعد في أنماط الاعتداءات الالكترونية، تبرز أهمية تبني إجراءات حديثة تقوم على التحليل الاســـتخباراتي المتقدم للمحتوى الرقمي، وتكامل الجهود بين الأجهزة الأمنية والجهات التقنية المختصة، وهي إجراءات لم يحظ تنظيمها بالاهتمام الكافي في التشريع الفلسطيني، في محاولة للوصول الى آليات فعالة قادرة على الوقاية من الاعتداءات الالكترونية التي قد تقع على أمن الدولة الداخلي والرصد المبكر لها.

الفرع الاول: التحليل الاستخباري للبيانات الرقمية

من ضـــمن الإجراءات التي باتت تُســـتخدم بكفاءة في مواجهة الاعتداءات الإلكترونية، يأتي التحليل الاستخباري للبيانات الرقمية، الذي يُقصد به دراسة سلوك الأفراد أو المجموعات عبر الإنترنت من خلال أدوات تحليل متقدمة تعتمد على الذكاء الاصطناعي والتعلم الآلي وأنظمة إدارة البيانات الكبرى.

فهي عملية تحويل المعلومات الخام الى معلومات اســـتخباراتية عملية، ففي مجال الامن، يجمع محللو الاستخبارات البيانات ويحللونها لإعداد تقارير استخباراتية موجزة، تساعد هذه التقارير في تحديد تهديدات الأمن الوطني (Augusta University, 2025)، كالإرهاب والجريمة المنظمة والتهديدات الالكترونية.

وتعتبر الاســتخبارات مفتوحة المصــدر من أبرز المصــادر التي يعتمد عليها المحللون في تحليل البيانات الرقمية، والتي من أهمها (Lindemulder & Forrest, 2025):

1. محركات البحث على الانترنت مثل: google.
2. وسائل الاعلام المطبوعة وعبر الانترنت بما في ذلك الصحف والمجلات والمواقع الإخبارية.

3. حسابات وسائل التواصل الاجتماعي مثل Facebook, X, Instagram, LinkedIn.

4. المنتديات عبر الانترنت والمدونات الالكترونية.

5. الشبكة المظلمة، وهي منطقة مشفرة من الانترنت لا يتم فهرستها بواسطة محركات البحث.

6. البيانات الفنية، مثل عناوين IP.

7. البحوث الاكاديمية بما في ذلك الأوراق والاطروحات والمجلات.

8. السجلات العامة.

وتكمن أهمية هذا الإجراء في قدرته على اكتشـــاف الحملات المنظمة، أو تحليل المنشـــورات التي تثير البلبلة، أو حتى كشف الجهات التي تُحرّك الخطاب الرقمي ضد الدولة، لكن تنفيذه يستلزم توفر تشريعات واضحة تحمي الخصوصية وتمنع الاستغلال السياسي أو الشخصي لهذه المعلومات. كما يتطلب بناء شراكة بين الأجهزة الأمنية والمؤسسات الأكاديمية أو الشركات التقنية المحلية، لتطوير أدوات تحليل فعالة.

هذا الإجراء لا يعتمد فقط على التدخل بعد وقوع الجريمة، بل يتخذ طابعًا استباقياً يمكن من خلاله رصد توجهات معينة أو أنماط محتوى مشبوهة أو علاقات بين مستخدمين قد تشير إلى وجود تنسيق يستهدف أمن الدولة. ورغم فاعلية هذا النوع من التحليل، إلا أنه لا يزال غائباً تقريباً في فلســـطين، ســـواء على المستوى التشريعي أو العملي، حيث تفتقر الأجهزة الأمنية إلى البنية التكنولوجية التي تسمح بتشغيل مثل هذه الأنظمة، كما لا يوجد طاقم متخصص يمكنه التعامل مع البيانات الضخمة أو استخراج المؤشرات منها. كما يجب إدراجه ضمن السياسات الجنائية حتى يصبح أداة قانونية معتمدة، مع النص على ضوابط استخدامه، وتحديد الجهات المخوّلة بتنفيذه، وكيفية توثيق نتائجه في ملفات التحقيق القضائي.

الفرع الثاني: التعاون بين القطاعين الأمني والتقني

من أبرز التطورات في مجال مواجهة الاعتداءات الإلكترونية هو إدراك أهمية التعاون بين الجهات الأمنية والمؤسسات التقنية، سواء كانت مزودي خدمة الإنترنت، أو شركات التكنولوجيا، أو حتى المطورين والمجتمع الرقمي المدني.

تشير الأدبيات الحديثة إلى أن الأمن السيبراني لم يعد مقتصراً على نطاق المؤسسات التقنية فقط، بل أصبح جزءاً لا يتجزأ من منظومة الأمن القومي للدول. وفقاً لمقال نُشر في CSO Online، فإن التهديدات السيبرانية أصبحت عابرة للقطاعات وتستهدف الأفراد والحكومات والشركات على حد سواء، الأمر الذي يجعل من المستحيل مواجهتها بجهة واحدة فقط. ويؤكد ان مواجهة هذا النوع من التهديدات يحتاج الى وجود التعاون بين القطاعين الأمني والتقني، وذلك من خلال تبادل المعلومات حول التهديدات السيبرانية بشكل لحظي، الأمر الذي يدعم قدرة الدولة على صياغة استراتيجيات استباقية للحماية من الهجمات (Security Staff, 2023).

في التشريع الفلسطيني، لا تزال العلاقة بين هذه الأطراف ليست واضحة بشكل كافي، وغالباً ما تفتقر إلى الأطر القانونية التي تُلزم الطرف التقني بالتعاون الفوري وتبادل المعلومات ضمن نطاق قانوني واضح. فبالرغم من ان القرار بقانون رقم 10 لسنة 2018 نص على التزامات مزودي الخدمة[1]، بتقديم ما يلزم من بيانات في كشف الحقيقة بناءً على طلب من النيابة العامة أو المحكمة المختصة، الا انها تبقى غير قادرة على الوقاية من وقوع الجريمة.

وفي محاولة لرفع وتعزيز الحماية من الهجمات والاعتداءات الالكترونية. تم تأسيس فريق الاستجابة لطوارئ الحاسوب (PALCERT) بموجب قرار مجلس الوزراء رقم 16 لسنة 2015، ويضم في عضويته 12 متخصصاً في مجال أمن المعلومات من مختلف المؤسسات الحكومية. في مجال الأمن السيبراني،

[1] المادة 51 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات.

يرمز CERT الى فريق الاستجابة لحالات الطوارئ الحاسوبية – وهو فريق من محللي أمن المعلومات المكلفين بالاستجابة لحوادث الأمن السيبراني وإدارتها داخل أي مؤسسة أو قطاع أو دولة. تشمل مهامهم الأساسية حماية الأنظمة، واكتشاف تهديدات الأمن السيبراني والتحقيق فيها، مثل خروقات البيانات أو هجمات رفض الخدمة، حيث تتجاوز مهمتهم مجرد الاستجابة للتهديدات، اذ يلعبون دوراً محورياً في منع المخاطر السيبرانية وتحليلها والتخفيف منها قبل أن تُسبّب أضراراً واسعة النطاق (Group-IB, n.d.).

ومن اهداف الفريق الأساسية التي جاءت في قرار مجلس الوزراء رقم 16 لسنة 2015[1]:

1. خلق بيئة معلوماتية حاسوبية فلسطينية آمنة وموثوقة ضمن أحدث وسائل التكنولوجيا المستخدمة.
2. بناء نقطة اتصال موثوقة من الكوادر الحكومية في أمن المعلومات الحاسوبية والاتصالات، بحيث يكون الفريق هو نقطة الاتصال المركزية الوطنية للتنسيق مع كافة الجهات المعنية.
3. بناء القدرات في مجال الأمن السيبراني لزيادة القدرة على كشف حوادث أمن المعلومات الحاسوبية والاستجابة لأي طارئ والرد على مثل هذه الحوادث.
4. تعزيز ثقافة الوعي في الأمن السيبراني في مؤسسات القطاع العام والخاص، بما في ذلك المواطنين.
5. إعداد سياسات وبرامج واستراتيجيات الأمن السيبراني والعمل على تنفيذها.
6. إيجاد بيئة تشريعية قانونية سليمة ناظمة للأمن السيبراني ومكافحة الجرائم الالكترونية، وذلك بما يتعلق بالجوانب الفنية والإدارية.
7. وضع الخطط التنفيذية والمالية للنهوض بعمل الفريق واستدامته.

ومع ذلك، لابد من استمرار الاستثمار في تطوير مهارات هذا الفريق، وتحديث ادواته التقنية، وتعزيز امكانياته العملية لضمان حماية البنية التحتية الوطنية من خطر التهديدات الالكترونية المتزايدة.

[1] المادة 4 من قرار مجلس الوزراء رقم 16 لسنة 2015 بالنظام الداخلي لعمل الفريق الفلسطيني للاستجابة لطوارئ الحاسوب.

كما لابد من إصـــدار قانون ينظم العلاقة بين القطاع الأمني والقطاع التقني في فلســـطين، يُحدد آليات مشاركة المعلومات، وفترات الاحتفاظ بالبيانات، وضمانات الحماية القانونية لجميع الأطراف، وإنشاء وحدة مشتركة أو لجنة تنسيقية تضم ممثلين عن الطرفين، تُعنى برصد المحتوى الرقمي الضار، والتعامل معه بطريقة فورية، وتحقيق الردع قبل تفاقم الأثر.

الخاتمة

لقد كشفت هذه الدراسة أن الاعتداءات الإلكترونية الموجهة ضد أمن الدولة الداخلي تمثل نمطاً جديداً من الجرائم المعاصرة التي تتسم بالتعقيد وسرعة التطور. فمع تطور أشكال الاعتداءات الإلكترونية، لم تعد النصوص القانونية التقليدية قادرة على مواكبة حجم التعقيد الذي بات يميز الفضاء الرقمي، سواء من حيث أدوات التنفيذ أو طبيعة الفاعلين أو حتى النطاق الزمني والجغرافي لتلك الأفعال. في هذا السياق، يظهر بوضوح أن القرار بقانون الفلسطيني رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية، رغم كونه من أهم الخطوات التي اتُخذت في سبيل تنظيم الفضاء السيبراني، قد وُضع في وقت كان فيه الوعي بمخاطر الأمن الرقمي لا يزال في بداياته، ما جعله يعالج أنواعًا معينة من الجرائم، كالتشهير أو التهديد أو الدخول غير المشروع، دون التطرق لصور مستحدثة أصبحت اليوم من أخطر ما يهدد امن المجتمع واستقراره.

وبالتالي، بينت هذه الدراسة ان هذا النوع من الاعتداءات يستدعي تفعيلاً للمنظومة التشريعية لسد الثغرات القائمة، وايضاً ضرورة تعزيز الدور المؤسسي لأجهزة العدالة بتبني آليات جديدة تتماشى مع البيئة الرقمية وبشكل يضمن تحقيق التوازن بين متطلبات حماية الأمن وضمان سيادة القانون.

وتوصلت هذه الدراسة الى جملة من النتائج والتوصيات وهي على النحو الآتي:

النتائج

1. تعرف الاعتداءات الالكترونية بأنها: " تلك التي تهدف إلى إلحاق الضرر بأنظمة المعلومات فتؤثر بذلك على سلامة المعلومات، ومصدر توافر المعلومات وسريتها في هذه الأنظمة، حيث ان هذه الاعتداءات تختلف درجة خطورتها باختلاف الدافع من الاعتداء، فمنها ما يكون بدافع سياسي، اقتصادي أو بدافع تجاري أو فردي ومنها من يقوم بالاعتداء من أجل الفضول والافتخار وغيرها من الاعتداءات".

2. يبرز الفارق بين "الاعتداء" و"الجريمة" في نطاق دراســتنا، أن كثيرًا من الأفعال لا تخضـــع لعقوبات قانونية صريحة، لعدم وجود نصوص تُجرّمها بشكل مباشر وبالتالي يُشار اليها بالاعتداء.

3. يكون أمن الدولة عرضـــة للخطر اما بطريقة تقليدية داخل المجتمع التقليدي كالاضـــطرابات واعمال الشـغب او اثارة عصـيان المسـلح وغيره، واما بطريقة الكترونية كالقيام بأي نشـاط الكتروني يهدد امن الدولة مثل التحريض على الفتنة او نشر الشائعات التي من شأنها أن تهدد الأمن الوطني عن طريق شـــبكات التواصـــل الاجتماعي، او الارهاب الالكتروني أو اختراق أنظمة معلوماتية تابعة للدولة أو تدميرها.

4. ان الإرهاب الالكتروني لا ينحصـــر في نمطاً واحداً من أنماط الســـلوك الجرمي، فقد يتكون من عدة أفعال، قد يشكل كل فعل منها جريمة مستقلة عادية وليس إرهابية، إلا أن ارتباطها بعناصـر الإرهاب وأهدافه وخطره تجعل من هذه الأفعال او الجرائم صوراً للجريمة الإرهابية.

5. تبيّن عجز النصوص التقليدية في القوانين النافذة عن مواجهة الجرائم الماسة بأمن الدولة الداخلي التي ترتكب بطريقة إلكترونية

6. ان قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 لم يتضمن احكاماً صريحة تتعلق بالجرائم الالكترونية رغم شموليته في تنظيم الإجراءات الجنائية التقليدية

7. تقع مسؤولية مكافحة الاعتداءات الالكترونية عدد من المؤسسات المعنية، في مقدمتها الشرطة ممثلة بوحدة الجرائم الإلكترونية، التي تضـطلع بمهمة تتبع الجرائم الرقمية والاعتداءات التي تسـتهدف الأمن العام والسـيادة الوطنية. كما يبرز دور الجهاز الوقائي وغيره من الأجهزة الأمنية في رصـد التحركات الرقمية ذات الطابع التحريضـــي أو الهدّام، وجمع الأدلة التقنية التي تُمكّن النيابة العامة من إقامة الدعوى الجنائية.

التوصيات

1. تعديل القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الالكترونية بما يضمن تأسيس باب مستقل فيه يضـــم كافة الأفعال التي تشـــكل اعتداءً يرتكب بطريقة الكترونية ويقع على أمن الدولة الداخلي، والتمييز بين أنماط السلوك الجرمي لكل منها.
2. تشديد العقوبات المترتبة على أي فعل يستهدف أمن الدولة الداخلي بالبيئة الالكترونية
3. تعزيز قدرات الأجهزة الأمنية المختصـــة وذلك من خلال تنظيم برامج تدريبية دورية تتناول الجوانب التقنية والقانونية للجرائم، بما يضـــمن رفع كفاءة الكوادر وتمكينها من التعامل بفعالية مع الاعتداءات التي تستهدف أمن الدولة الداخلي في الفضاء الالكتروني.
4. تحديث البنية التحتية الوطنية لتقنية المعلومات والاتصـــالات، لتعزيز كفاءتها في الحماية من الاختراقات والاعتداءات الالكترونية.
5. الاستثمار في فريق الاستجابة لطوارئ الحاسوب في فلسطين وتعزيز قدراته العملية في مجال الحماية من التهديدات الالكترونية على قواعد البيانات الحكومية.

المراجع العلمية

المراجع العربية:

القرآن الكريم.

إبراهيم، خالد ممدوح. (2008). *أمن الجريمة الإلكترونية*. الإسكندرية، مصر: الدار الجامعية.

إبراهيم، خالد ممدوح. (2009). *الجرائم المعلوماتية*. الإسكندرية: دار الفكر الجامعي.

ابن منظور، محمد بن مكرم. (2000). *لسان العرب* (الإصدار الطبعة الأولى). بيروت: دار صادر.

ابو الحسين، احمد بن فارس بن زكريا. (د.ت.). معجم *مقاييس اللغة*. بيروت: دار الفكر.

أبو العطا، مجدي محمد. (2016). *أمن المعلومات والإنترنت* (الإصدار الطبعة الأولى). القاهرة، مصر: شركة علوم الحاسبة (كمبيوساينس).

أبو زهرة، محمد. (1998). *الجريمة والعقوبة في الفقه الإسلامي*. القاهرة: دار الفكر العربي.

ابو غليون، عطوة مضعان. (2009). *الجرائم الالكترونية بين الشريعة الاسلامية والقوانين الوضعية*، رسالة ماجستير، 64. عمّان، الأردن: الجامعة الأردنية.

الاتفاقية الدولية لقمع تمويل الإرهاب المعتمدة والمعروضة للتوقيع والتصديق بموجب قرار الجمعية العام رقم 54–109 المؤرخ في 9 كانون الأول/ديسمبر 1999.

الاتفاقية العربية لمكافحة الارهاب لسنة 1998.

الإدريسي، علي يوبي. (2018). *الشرطة القضائية في مسرح الجريمة سلطات وقيود، رسالة ماجستير*، 16. فاس، المغرب: جامعة سيدي محمد بن عبد الله، كلية العلوم القانونية الاقتصادية والاجتماعية.

الأكاديمية العربية للعلوم المالية والمصرفية. (31 8، 2016). *مسرح الجريمة والتحقيق فيها*. تم الاسترداد من http://www.aabfs.org/ar

الأمم المتحدة. (10–17 نيسان 2000). *المؤتمر العاشر لمنع الجريمة ومعاقبة المجرمين*. المؤتمر العاشر لمنع الجريمة ومعاقبة المجرمين. فيينا، النمسا: الأمم المتحدة.

باطلي، غنية. (2015). *الجريمة الإلكترونية*، الطبعة الأولى (الإصدار الطبعة الاولى). الجزائر: منشورات الدار الجزائرية.

بن سليمان، حصة عبد الله. (2013). دور مجلس التعاون الخليجي في مكافحة الاتجار بالبشر، *رسالة دكتوراه*، 20. القاهرة، مصر: كلية الاقتصاد والعلوم السياسية.

بن يونسن عمر. (2004). *الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه*، 649. مصر: كلية الحقوق في جامعة عين شمس.

بهنام، رمسيس. (1990). *جرائم الاعتداء على المصلحة العمومية*. الإسكندرية: منشأة المعارف.

الجرجاني، علي بن محمد بن علي الزين الشريف. (1983). *التعريفات* (الإصدار الطبعة الأولى). بيروت، لبنان: دار الكتب العلمية.

الجزيرة. (04 06، 2025). قراصنة "جبروت" يستولون على 4 تيرابايتات من قاعدة بيانات السجل العقاري في المغرب. تم الاسترداد من الجزيرة نت: https://www.aljazeera.net/tech/2025/6/4/قراصنة-جبروت-يستولون-على-4-تيرابايتات

حجازي، عبدالفتاح بيومي. (2002). *الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت*. القاهرة، مصر: دار الكتب القانونية.

الحديثي، فخري، و الزعبي، خالد. (2010). *القسم الخاص في قانون العقوبات* (الإصدار الطبعة الثانية). عمان، الأردن: دار الثقافة.

حديد، نوفيل، و مسوس، كمال. (2016). مقاربات حماية أنظمة معلومات المؤسسة من الاعتداءات الإلكترونية. المؤسسة(05)، 33.

حكم محكمة القضاء الإداري المصري الصادر في الدعوى رقم 21855 لسنة 65 قضائية، 21855 لسنة 65 قضائية (محكمة القضاء الاداري المصرية 28 5، 2011).

الحمادي، عيسى محمد عبد الله. (10، 2018). *قمع تمويل الارهاب في القانون الدولي- دراسة مقارنة، رسالة ماجستير*، 24. العين (امارة ابو ظبي)، الإمارات العربية المتحدة: كلية القانون، جامعة الامارات العربية المتحدة.

الحمامي، حسين، و الحكيم، مازن سمير. (2017). *كل شيء عن إنترنت الأشياء وتطبيقات المدن الذكية* (الإصدار الطبعة الأولى). الأردن: دار الراية.

حومد، عبد الوهاب. (1975). *شرح قانون الجزاء الكويتي – القسم العام*. الكويت: مطبوعات جامعة الكويت.

الخشت، محمد عثمان. (1996). *الشائعات وكلام الناس*. مصر: مكتبة ابن سينا.

الخطيب، باسل مصطفى، و وآخرون. (2016). *الحاسوب والبرمجيات الجاهزة: مهارات الحاسوب* (الإصدار الطبعة الأولى). عمان، الأردن: دار الاعصار العلمي.

خلفي، عبد الرحمن. (2010). *محاضرات في قانون الإجراءات الجزائية*. الجزائر: دار الهدى.

خميخم، محمد. (30 6، 2020). موقف التشريع الجزائري من جريمة الإرهاب الإلكتروني. *مجلة حوليات جامعة الجزائر، 34*(2)، 35.

الخولي، أحمد محمد فتحي. (10، 2021). المسؤولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي "الديب فيك نموذجاً". *مجلة البحوث الفقهية والقانونية*، (36)، 252.

الرشيد، غازي عبد الرحمن هيان. (2004). *الحماية القانونية من جرائم المعلوماتية (الحاسب والانترنت)، اطروحة دكتوراه*، 106. لبنان: الجامعة الاسلامية في لبنان، كلية الحقوق.

رمضان، مدحت. (2001). *الحماية الجنائية للتجارة الإلكترونية*. القاهرة، مصر: دار النهضة العربي.

الزنط، سعد عطوة. (2010). الارهاب الالكتروني وإعادة صياغة استراتيجيات الأمن القومي. *مؤتمر الجرائم المستحدثة – كيفية اثباتها ومواجهتها* (صفحة 2). المركز القومي للبحوث الاجتماعية والجنائية.

زهران، سحر جمال. (2019). الجوانب القانونية الدولية لجريمة الإرهاب الالكتروني. *مجلة كلية السياسة والاقتصاد*، (4)، 79.

السراج، عبود. (1995). *قانون العقوبات السوري* – القسم العام. دمشق: جامعة دمشق.

السراج، عبود. (1999). *شرح قانون العقوبات* – القسم العام (الإصدار ط9). سوريا: مطبعة الجامعة.

السنباطي، إيهاب. (19–20 يونيو 2007). *"ماهية الجريمة الإلكترونية – المفهوم والخصائص"*، ورقة بحث. الندوة الإقليمية حول الجرائم المتصلة بالكمبيوتر. الدار البيضاء.

السنوسي، عبد الله محمد. (فبراير، 2018). الاشتراك المانع من القصاص في جريمة القتل العمد (دراسة مقارنة). *مجلة الشريعة والقانون، 15*(31)، 14.

شاكر، حميد عبد العزيز محمد، و دقاني، خالد محمد. (2022). احكام التجريم والجزاء لترويج الشائعات والأخبار الماسة بأمن الدولة والنظام العام عبر وسائل التواصل الاجتماعي في التشريع الاماراتي. *مجلة جامعة الشارقة للعلوم القانونية، 19*(4)، 51.

شمس الدين، أشرف توفيق. (2007). *الحماية الجنائية للحرية الشخصية من الوجهة الموضوعية "دراسة مقارنة"* (الإصدار 2). القاهرة: دار النهضة العربية.

الشواربي، عبد الحميد. (1997). *جرائم الصحافة والنشر وقانون حماية حق المؤلف والرقابة على المصنفات الفنية في ضوء القضاء والفقه* (الإصدار ط2). الإسكندرية، مصر: منشأة المعارف.

الشواربي، عبد الحميد. (2003). *التعليق الموضوعي على قانون العقوبات – الأحكام العامة لقانون العقوبات في ضوء الفقه والقضاء* (الكتاب الأول). الإسكندرية: منشأة المعارف.

الصيفي، عبد الفتاح مصطفى. (1967). *القاعدة الجنائية: دراسة تحليلية لها على ضوء الفقه الجنائي المعاصر*. القاهرة: دار النهضة العربية.

العادلي، محمود صالح. (2006). *الجرائم المعلوماتية ماهيتها وصورها. ورشة العمل الإقليمية حول: تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية*، (صفحة 5). مسقط.

عالية، سمير. (1999). *الوجيز في شرح الجرائم الواقعة على أمن الدولة، دراسة مقارنة* (الإصدار ط1). بيروت: المؤسسة الجامعية للدراسات والنشر.

عبد الحكيم، توات. (2021). جريمة الإرهاب الالكتروني، *رسالة ماجستير*، 33. تبسة، الجزائر: جامعة العربي التبسي.

عبد الحكيم، مولاي ابراهيم. (2015). الجرائم الإلكترونية. *مجلة الحقوق والعلوم الإنسانية*، (23)، 213.

عبد الهادي، عبد العزيز مخيمر. (1986). *الإرهاب الدولي*. القاهرة: دار النهضة العربية.

العبيدي، أسامة بن غانم. (ديسمبر، 2013). التفتيش عن الدليل في الجرائم المعلوماتية. *المجلة العربية للدراسات الأمنية والتدريب، 29*(58)، 87.

العجلان، عبد الله بن عبد العزيز. (2008). *الإرهاب الإلكتروني في عصر المعلومات. المؤتمر الدولي الأول حول " حماية أمن المعلومات والخصوصية في قانون الانترنت"*، (صفحة 19). القاهرة.

عرفة، محمد السيد. (2013). *الاتفاقية الدولية لقمع تمويل الإرهاب ومدى فاعليتها في مكافحته، دراسة تأصيلية تحليلية مقارنة*، 9. الرياض: جامعة نايف العربية للعلوم الأمنية.

العريشي، جبريل بن حسن، و الشلهوب، محمد حسن. (2016). *أمن المعلومات* (الإصدار الطبعة الأولى). عمان، الأردن: دار المنهجية.

عطية، أيسر محمد. (2014). *دور الآليات الحديثة للحد من الجرائم المستحدثة وطرق مواجهته*. ملتقى دولي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، (صفحة 9).

العقات، نظمي توفيق. (2012). *القسم الخاص في قانون العقوبات* (الإصدار الطبعة الثالثة). الأردن: دار الثقافة للنشر والتوزيع.

عمارة، فوزي. (جوان، 2010). اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية. *مجلة العلوم الإنسانية*، (33)، 236.

عمايره، رضية أحمد. (2025). المسؤولية الجزائية لنشر الأخبار الكاذبة بالوسائل الالكترونية. *مجلة جامعة الزيتونة الأردنية للدراسات القانونية، 6*(2)، 166.

عياد، سامي علي حامد. (2007). *الجريمة المعلوماتية وجرائم الانترنت*. مصر: دار الفكر الجامعي.

غلاب، أحمد، و كيسي، زهيرة. (يناير، 2019). إجراءات اعتراض المكالمات السلكية واللاسلكية كآلية لمتابعة جرائم المخدرات. *مجلة تحولات*، 2(1)، 273.

فريق المركز السوري للأمن الرقمي. (28 06، 2025). *تقرير عام: تسريب واسع لبيانات رسمية سورية عبر الإنترنت والمنتديات المظلمة*. تم الاسترداد من المركز السوري للأمن الرقمي: https://ar.sysoc.net/blog/leaks-2025

الفقي، عبد الحليم فؤاد. (2020). جريمة نشر الأخبار والشائعات الكاذبة في القانون المصري. *الباحث العربي، 1*(2)، 84.

قاموس المعاني. (د.ت.). *قاموس عربي عربي*. تم الاسترداد من المعانيhttps://www.almaany.com :

قانون الإجراءات الجزائية الفلسطيني رقم (3) لسنة 2001.

القانون الأساسي المعدل.

قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

قانون الجرائم الالكترونية الأردني رقم 17 لسنة 2023.

قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018.

قانون منع الإرهاب الأردني رقم 55 لسنة 2006.

القرار الصادر عن محكمة صلح جزاء عمان رقم 2023/19411.

القرار الصادر عن محكمة صلح جزاء عمان رقم 2023/22600.

القرار الصادر عن محكمة صلح جزاء عمان، رقم 2023/19411 (محكمة صلح جزاء عمان 2023).

القرار الصادر من مجلس الوزراء رقم 16 لسنة 2015 (المتعلق بالنظام الداخلي لعمل الفريق الفلسطيني للاستجابة لطوارئ الحاسوب).

القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية.

قرار بقانون رقم 39 لسنة 2022 بشأن مكافحة غسل الاموال وتمويل الإرهاب.

قرار محكمة القضاء الإداري المصري الصادر في الدعوى رقم 21855 لسنة 65 القضائية.

قرارية، أحمد معروف. (2017). سلطات ماموري الضبط القضائي في التشريع الجزائي الفلسطيني، *رسالة ماجستير*، 26–29. نابلس، فلسطين: كلية الدراسات العليا، جامعة النجاح الوطنية.

كردي، احمد السيد. (30 09، 2011). أمن المعلومات ماهيتها وعناصرها واستراتيجياتها. تاريخ الاسترداد 01 04، 2024، من كنانة أونلاين : http://kenanaonline.com/users/ahmedkordy/posts/323552

كميل، المقدم جهاد. (11 11، 2024). *مقابلة اجرتها الباحثة مع مدير المباحث في جهاز الشرطة الفلسطيني*. (أسيل البكري، المحاور) نابلس.

اللبيدي، ابراهيم محمود. (2010). *الحماية الجنائية لأمن الدولة*. القاهرة، مصر: دار الكتب القانونية.

المبارك، عبدالله يحيى. (د.ت.). *أهمية أمن المعلومات*. تم الاسترداد من مركز التميز لأمن المعلومات : http://www.coeia.edu.sa

محلق، جميلة. (جوان، 2015). اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية الجزائري. *مجلة التواصل في الاقتصاد والإدارة والقانون*، (42)، 178.

محمود، عبد الله ذيب، و دراج، أسامة إسماعيل. (2022). *الوجيز في الجرائم الإلكترونية* (الإصدار الطبعة الأولى). عمان، الأردن: دار الثقافة.

المرسوم بقانون اتحادي رقم 34 لسنة 2021 بشأن مكافحة الشائعات والجرائم الالكترونية.

مرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية رقم 34 لسنة 2021. (بلا تاريخ). المادة 1 من مرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية رقم 34 لسنة 2021 .

المرسوم بقانون بشأن مكافحة الشائعات والجرائم الالكترونية. (2021).

مصطفى، احمد محمود. (2010). *جرائم الحاسبات الالية في التشريع المصري "دراسة مقارنة"* (الإصدار الطبعة الأولى). مصر: دار النهضة العربية.

الملط، احمد خليفة. (2006). *الجرائم المعلوماتية* (الإصدار الطبعة الثانية). الإسكندرية: دار الفكر الجامعي.

مناصرة، عبد الله. (1991). *الاستخبارات العسكرية في الإسلام* (الإصدار الطبعة الثانية). بيروت، لبنان: مؤسسة الرسالة.

مهدي، عبد الرؤوف. (2011). *شرح القواعد العامة لقانون العقوبات*. القاهرة: دار النهضة العربية.

الموسوعة العربية العالمية. (د.ت). *الالكترونيات* (المجلد 2). الرياض: مؤسسة أعمال الموسوعة للنشر والتوزيع.

نابلسي، علاء الدين. (2020). *السياسة الجنائية في مواجهة جرائم التجسس "دراسة مقارنة"، رسالة ماجستير*، 19. نابلس، فلسطين: كلية الدراسات العليا، جامعة النجاح الوطنية.

نجم، محمد صبحي. (2000). *قانون العقوبات: القسم العام* (النظرية العامة للجريمة) (الإصدار الطبعة الأولى). عمان: دار الثقافة للنشر والتوزيع.

النوايسة، عبد الاله محمد. (09، 2005). التكييف الجرمي لتمويل الإرهاب، دراسة في التشريع الأردني. *مجلة دراسات الشريعة والقانون*، (24)، 344.

النوايسة، عبد الإله محمد. (2005). *الجرائم الواقعة على أمن الدولة في التشريع الأردني*. عمان: دار وائل للنشر.

الهاجري، إياس. (ب. ت.). *جرائم الإنترنت*. تم الاسترداد منwww.arabcin.net/gold

هباس بن رجاء الحربي. (2012). الشائعات ودور وسائل الإعلام في عصر المعلومات، . عمان، الأردن: دار أسامة للنشر والتوزيع.

هدى قشقوش. (1992). جرائم الحاسب الالكتروني في التشريع الموازن. القاهرة: دار النهضة العربية.

الهروي، محمد بن أحمد بن الأزهري. (2001). *تهذيب اللغة* (الإصدار الطبعة الأولى). بيروت، لبنان: دار إحياء التراث العربي.

هلالي عبد اللاه احمد. (2007). جرائم المعلوماتية عابرة الحدود. القاهرة: دار النهضة العربية.

الهيتي، محمد حماد. (يوليو/ جمادي الثانية، 2006). البحث عن حماية جنائية للبيانات والمعلومات الشخصية. *مجلة الشريعة والقانون*، (27)، 427.

وردة شرف الدين. (جوان، 2017). مشروعية أساليب التحري الخاصة المتبعة في مكافحة الجريمة المعلوماتية – في التشريع الجزائري –. مجلة المفكر(15)، 543.

وزارة الأوقاف والشؤون الإسلامية–الكويت. (1984). الموسوعة الفقهية الكويتية (الإصدار الطبعة الثالثة). الكويت: وزارة الأوقاف والشؤون الإسلامية.

يسر أنور علي. (د.ت.). شرح النظريات العامة للقانون الجنائي .

يوسف المصري. (2011). الجرائم المعلوماتية والرقمية للحاسوب والانترنت (الإصدار الطبعة الأولى). مصر: دار العدالة.

يوسف شحادة. (1999). الضابطة العدلية – علاقتها بالقضاء ودورها في سير العدالة الجزائية. بيروت: مؤسسة بحسون.

المراجع الاجنبية

Augusta University. (2025). *Types of Intelligence Analysis.* Retrieved from Augusta University: https://www-augusta-edu.translate.goog/online/blog/types-of-intelligence-analysis?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=rq

Baize, D. (1999, juin-juillet-aout). De la contrefaçon à l'imitation. *Revue française de gestion*, 76-78.

Brooks, T., & et al. (n.d.). *Increasing Threats of Deepfake Identities.* U.S. Deppartment of Homeland Security. U.S. Deppartment of Homeland Security.

Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review, 107*, 1777.

Dobber, T., Metoui, N., Trilling, D., Helberger, N., & Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *International Journal of Press/Politics, 26*(1), 70.

Engler, A. (2019). *Fighting deepfakes when detection fails.* Brookings Institution. Brookings Institution.

Forester, T. (1989). *Essential Problems to High-Tech Society* (First Edition ed.). Cambridge, Massachusetts: MIT Press.

Group-IB. (n.d.). *CERT.* Retrieved from Group-IB Resources/Knowledge Hub: https://www.group-ib.com/resources/knowledge-hub/cert/

Hancock, J., & Bailenson, J. (2021). The Social Impact of Deepfakes. *Cyberpsychology, Behaviour, and Social Networking, 24*(3), 151.

K. Tiedemann .(1989) .Fravde et Aetersd Affairs Commise al Aideordinateurseleronigues. .*Rev. Dry Pen. Crim*.612 ،

Lindemulder, G., & Forrest, A. (2025). *What Is Open Source Intelligence (OSINT)?* Retrieved from IBM Think: https://www.ibm.com/think/topics/osint#How+OSINT+works.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing* (5th ed.). Pearson Education, Inc.

Security Staff. (2023, March 27). *Public-Private Partnerships are Essential to Strengthen Cybersecurity Globally.* Retrieved from CSO Online: . https://www.csoonline.com/article/574891/public-private-partnerships-are-essential-to-strengthen-cybersecurity-globally.html.

Thomson, D. (1991). Current Trends in Computer Crime. *Computer Control Quarterly, 9*(1), 2.

An-Najah National University
Faculty of Graduate Studies

CYBER-ATTACKS ON INTERNAL SECURITY AND THE ROLE OF THE CRIMINAL JUSTICE SYSTEM IN COMBATING THEM

By
Aseel Ayman "Mohammed Kamal" Albakri

Supervisors
Dr. Fadi Shadid
Dr. Abdullah Mahmmoud

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Criminal Law, Faculty of Graduate Studies, An-Najah National University, Nablus - Palestine.
2025

CYBER-ATTACKS ON INTERNAL SECURITY AND THE ROLE OF THE CRIMINAL JUSTICE SYSTEM IN COMBATING THEM

By
Aseel Ayman "Mohammed Kamal" Albakri
Supervisors
Dr. Fadi Shadid
Dr. Abdullah Mahmmoud

Abstract

This thesis examines the issue of cyber-attacks on the national security of Palestine, recognizing it as an emerging challenge that increasingly confronts legislators and relevant authorities amid rapid technological advancements. The expanding reliance on technology across diverse sectors has facilitated the emergence of novel forms of cybercrime targeting information infrastructures and governmental websites, thereby directly impacting state stability and societal security.

This study aims to elucidate the electronic security threats that may impact national security through the internet. The primary focus of the research is to identify actions that constitute attacks on national security when perpetrated via electronic networks, as well as to examine how the Palestinian legislature and relevant authorities have addressed these issues. Additionally, the study seeks to highlight deficiencies within Palestinian criminal legislation by comparing it with legislative frameworks from other Arab countries, with the intention of deriving potential improvements.

The study concludes that safeguarding national security in cyberspace necessitates the revision of legal frameworks governing cybercrimes in Palestine to align with technological advancements. Additionally, it emphasizes the importance of enhancing the capabilities of relevant security authorities by providing them with sophisticated digital investigation tools. Effective countermeasures against cyber-attacks also require the development of practical and technical procedures tailored to the specific nature and complexity of these threats, ensuring prompt response and precise evidence collection. These measures collectively strengthen the security system's capacity to address cybercrimes and maintain the stability of the state and society.

Keywords*:* cyber-attacks, national security, cybercrime, information infrastructures, digital investigation tools, Palestinian legislature