أكاديمية الشرطة
Police Academy

وزارة الداخلية
Ministry of Interior
State of Qatar • دولة قطر

مجلة الدراسات القانونية والأمنية

JOURNAL OF LEGAL AND SECURITY STUDIES

مجلة علمية دورية محكمة نصف سنوية تصدر عن مركز البحوث والدراسات الأمنية - أكاديمية الشرطة
Semi-Annual Peer-Reviewed Scientific Journal Issued By The Centre For Security Research And Studies Police Academy

Vo.5 - No.2 - July 2025 المجلد 5 - العدد 2 - يوليو 2025

ISSN 2789-1518

المجلد 5 - العدد 2 - يوليو 2025
Vol. 5, No.2 - July 2025

محتويات العدد

كلمة العدد 3

شروط وأخلاقيات النشر بالمجلة 5

البحوث والدراسات

البحوث والدراسات باللغة العربية

المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي (دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل الأدلة الرقمية)
الأستاذ الدكتور/ حسام نبيل الشنراقي
أستاذ علوم الشرطة - رئيس قسم إدارة الشرطة - أكاديمية شرطة دبي 11

التحديات الأمنيّة التي تواجه الأمن البحريّ في الخليج العربيّ وتأثيرها وانعكاساتها على حركة الملاحة البحريّة
الدكتور/ محمد علي محمد ابوشامة
كبير محاضرين علوم بحرية
الإدارة العامة لأمن السواحل والحدود
حافظ عبدالرحمن عبدالله عبدالرحمن
محاضر علوم بحرية أول
الإدارة العامة لأمن السواحل والحدود 67

دور الحوار والتفاوض في إدارة التظاهرات
الدكتور/ أيمن سعدالدين عبدالرحيم
الأستاذ المشارك بقسم إدارة الشرطة - أكاديمية شرطة دبي 137

جرائم غسل الأموال وأوجه خروجها عن الأحكام العامة في القانون القطري
الدكتور/ إياد هارون الدوري
أستاذ القانون الجنائي المساعد - كلية القانون - جامعة قطر 195

حجيّة الأحكام الجنائيّة أمام سلطات التأديب
دراسة تحليليّة مقارنة بين القانون القطريّ والقانون المصريّ
مريم عبدالله العون
ماجستير في القانون العام - جامعة قطر / باحث قانوني في مجلس التأديب الابتدائي - وزارة الداخلية، قطر 227

Researches & Studies In English

Terms and Ethics of Publication I-VIII

Factors Affecting Cyberbullying, Cyberbullying Victimization and Cyberbullying Perpetration Among College Students
Professor Dr. Dhiab Al-Badayneh
Professor of Methodology, Criminology and Forensic Psychology
Faculty member at the graduate studies department at Police Academy, Qatar 263

Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar
Abdulrahman Mohammed M SH Al-Shafi
Masters of Public Policy (HBKU) - Director of Cyber Strategies and Policies Department
National Cyber Security Agency (NCSA) 291

وزارة الداخلية
Ministry of Interior
State of Qatar - دولة قطر
أكاديمية الشرطة
Police Academy

مجلة الدراسات القانونية والأمنية
JOURNAL OF LEGAL AND SECURITY STUDIES

مجلة علمية دورية محكمة نصف سنوية تصدر عن
مركز البحوث والدراسات الأمنية - أكاديمية الشرطة

ISSN 2789-1518

المشرف العام
العقيد د./ جاسم محمد الخميس العبيدلي
مدير مركز البحوث والدراسات الأمنية

نائب المشرف العام
الرائد د./ خليفة أحمد بوهاشم السيد
مساعد مدير مركز البحوث والدراسات الأمنية

رئيس التحرير
أ.د./ عادل يحيى قرني علي

مدير التحرير
الرائد/ محمد راشد الدوسري
رئيس قسم الإصدارات العلمية بمركز البحوث والدراسات الأمنية

هيئة التحرير
أ.د./ عمرو إبراهيم الوقاد
أ.د./ مخلد ارخيص الطراونة
أ.د./ خالد محمد الحلبي
أ.د./ أناس عبدالعزيز المشيشي
د./ عبد الناصر عباس عبد الهادي
د./ عبدالرؤوف بن هادي اللومي
د./ عبدالصمد عبدالعزيز سكر

سكرتارية التحرير
كمال الدين حسن الإمام

التصميم والإخراج الفني
محمد عمر شحرور

الترجمة
جمال محمد الشرفي

التدقيق اللغوي
د. مصطفى أصلان
محمد سمير الجيلاني

الطباعة
مطابع الشرطة - دولة قطر

للتواصل
هاتف: 2356049 974+
بريد إلكتروني: pcjlss@moi.gov.qa

مجلة
الدراسات القانونية والأمنية
JOURNAL OF LEGAL AND SECURITY STUDIES

الهيئة الاستشارية

سعادة اللواء الدكتور
عبدالله يوسف المال
المستشار القانوني لسعادة وزير الداخلية
المشرف العام على أكاديمية الشرطة

سعادة السيد
سلطان بن عبدالله السويدي

اللواء الدكتور
ناصر بن سعيد آل فهيد الهاجري
مستشار رئيس جهاز أمن الدولة

اللواء
عبدالرحمن ماجد آل شاهين السليطي
رئيس أكاديمية الشرطة
وزارة الداخلية

الدكتور
إبراهيم عبد الله الأنصاري
عميد كلية الشريعة والدراسات الإسلامية
جامعة قطر

الدكتور
طلال عبدالله العمادي
جامعة قطر

المقدم الدكتور
جاسم خالد جاسم الحمر
مساعد مدير عام الاتصالات ونظم المعلومات
وزارة الداخلية

كلمة العدد

بحمد الله وفضله، تواصل مجلة الدراسات القانونية والأمنية أداء رسالتها العلمية بكل مهنية وانتظام، مؤكدة التزامها الثابت بأن تكون منبرًا رصينًا لنشر المعرفة المتخصصة في حقلي القانون والأمن. لقد استطاعت المجلة، على مدى سنوات صدورها، أن ترسخ مكانتها بوصفها إصدارًا علميًا محكّمًا يُعنى بتقديم أبحاث ذات جودة عالية، تعكس روح الاجتهاد الأكاديمي وتسهم في تعميق الفهم حول القضايا القانونية والأمنية الراهنة.

وفي ظل التغيرات المتلاحقة التي يشهدها العالم المعاصر – سواء في بنيته التقنية أو في تفاعلاته السياسية والاجتماعية – تبرز الحاجة الماسّة إلى تجديد الفكر القانوني والأمني، وتطوير أدوات التحليل والمعالجة بما يواكب تلك التحولات. من هنا، تبرز أهمية الأبحاث والدراسات الجادة التي تسلط الضوء على هذه التحديات وتقدّم حلولاً مدروسة تستند إلى منهج علمي رصين.

ويأتي صدور هذا العدد تزامنًا مع مرور خمس سنوات على انطلاق المجلة، وهي محطة نوعية تُجسّد ثمرة الجهود التراكمية التي بذلها فريق العمل في مركز البحوث والدراسات الأمنية بأكاديمية الشرطة بالتعاون مع هيئة تحرير المجلة، حيث تم – بحمد الله – تدشين النظام الآلي لمجلة الدراسات القانونية والأمنية وذلك في إطار العمل على تطوير وأتمتة تقديم الأبحاث والدراسات ونشرها بالمجلة، والعمل على الارتقاء بتصنيف المجلة محليا ودوليا. وقد التزمت المجلة، منذ إصدارها الأول، بأعلى معايير التحكيم العلمي، وحرصت على اختيار الأعمال البحثية التي تجمع بين الأصالة والمنهجية العلمية.

ويضم هذا العدد نخبة من الأبحاث العلمية التي تتناول موضوعات راهنة تهم المشتغلين في الشأنين القانوني والأمني، ففي المجال القانوني اشتمل العدد على دراستين تتناولان «جرائم غسل الأموال وأوجه خروجها عن الأحكام العامة في القانون القطري»، و«حجيّة الأحكام الجنائيّة أمام سلطات التأديب – دراسة تحليليّة مقارنة بين القانون القطريّ والقانون المصريّ». وفي المجال الأمني تناول العدد «المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي: دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل

الأدلة الرقمية»، و«التحديات الأمنيّة التي تواجه الأمن البحريّ في الخليج العربيّ وتأثيرها وانعكاساتها على حركة الملاحة البحريّة»، بالإضافة إلى بحث حول «إدارة التظاهرات من خلال أسلوبي الحوار والتفاوض».

كما اشتمل العدد على بحثين باللغة الإنجليزية الأول بعنوان:

«Factors Affecting Cyberbullying, Cyberbullying Victimization, and Cyberbullying Perpetration Among College Students»

والبحث الثاني بعنوان :

«Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar»

وتغتنم هيئة تحرير المجلة هذه المناسبة لتعرب عن بالغ امتنانها لكل الجهات التي كان لها دور فاعل في إنجاز هذا العدد، وفي مقدمتها أقسام مركز البحوث والدراسات الأمنية، ووحدة العلاقات العامة بأكاديمية الشرطة، وإدارة العلاقات العامة بوزارة الداخلية، بالإضافة إلى مطابع الشرطة.

كما تدعو الهيئة كافة الباحثين والخبراء إلى الإسهام بأعمالهم البحثية في أعداد المجلة القادمة، بما يعزز من رصيدها المعرفي ويكرّس حضورها كمرجع موثوق يواكب تطورات المعرفة في مجالي القانون والأمن، ويستجيب لمتطلبات البحث الأكاديمي الرصين.

شروط و أخلاقيات النشر بالمجلة

أولاً: شروط النشر بالمجلة

ترحب المجلة بنشر البحوث والدراسات باللغات العربيَّة والإنجليزيَّة والفرنسيَّة وفقًا للقواعد والضوابط الآتية:

1) ألاّ يكون البحث المقدم للنَّشر قد سبق نشره بأية وسيلة نشر، وألاّ يتم تقديمه لأيَّة جهة نشر أخرى أثناء فترة تحكيمه، ويتعهد الباحث بذلك خطيًّا.

2) أن يتسم البحث بالحداثة، والمنهجيَّة العلميَّة، مع سلامة اللُّغة، والمقارنة بالقانون القطريّ كلَّما كان ذلك ممكنًا.

3) ألاّ يتجاوز عدد صفحات البحث أو الدِّراسة (40) صفحة، ورغم ذلك يجوز لهيئة تحرير المجلَّة- بصفة استثنائيَّة- أن تتجاوز عن هذا الشَّرط إذا كانت طبيعة موضوع البحث أو الدِّراسة تقتضي ذلك.

4) أن يرسل الباحث سيرته الذاتيَّة الحديثة على أن تتضمن درجته العلميَّة.

5) تكون الأولويَّة في النشر للبحوث والدِّراسات القانونيَّة والأمنيَّة المقبولة للنشر بحسب أسبقيَّة ورود تقارير المحكمين بصلاحيتها للنشر.

6) لهيئة التحرير استبعاد أي بحث أو دراسة مخالفة لقواعد النَّشر بالمجلَّة، أو مقتضيات المصلحة العامَّة.

7) يخضع ترتيب البحوث والدراسات المقبولة للنشر في أعداد المجلة لاعتبارات الملاءمة التي تقدرها هيئة التحرير.

8) تعبر البحوث والدِّراسات التي تنشر في المجلَّة عن آراء أصحابها ولا تمثل رأي المجلَّة، ويتحمل صاحب البحث أو الدِّراسة المسؤوليَّة القانونيَّة عن ذلك.

9) لا ترد البحوث أو الدِّراسات المرسلة للمجلة إلى أصحابها، سواءً قبلت للنَّشر في المجلَّة أم لم تقبل.

ثانياً: أخلاقيات النشر:

تتبنى المجلة معايير أخلاقيات البحث والنشر العلمي، وفي ضوء هذه المعايير يتعين:

1) ألاّ يكون البحث المقدم للنَّشر قد سبق نشره بأية وسيلة نشر، وألاّ يتم تقديمه لأيَّة جهة نشر أخرى أثناء فترة تحكيمه، ويتعهد الباحث بذلك خطيًّا.

2) ألاّ يكون البحث أو الدِّراسة جزءًا من رسالة ماجستير أو رسالة دكتوراه سبق أن أعدَّها الباحث، أو جزءًا من كتاب سبق له نشره، أو أي عمل آخر منشور حفاظًا على حقوق الملكيَّة الفكريَّة.

3) الالتزام بقواعد البحث العلمي وأصوله من حيث منهجيَّة التَّقسيم، وقواعد التَّوثيق المرجعي، والأمانة العلميَّة، وأن يتضمن البحث خاتمة تشتمل على خلاصة البحث ونتائجه والتَّوصيات المقترحة، وأن يكون مصحوبًا بقائمة المراجع التي اعتمد عليها الباحث.

4) يعد تقديم البحث للنشر في المجلة موافقة ضمنية على السماح للمجلة بإتاحة البحث في أي شكل وفي أي قاعدة بيانات أو مستودع رقمي دون الرجوع للباحث.

5) إذا تعدد الباحثون في بحث واحد أو دراسة واحدة، وجب تحديد نطاق وطبيعة الإسهامات الفرديَّة لكل منهم. ويجب أن يكون لكل باحث يثبت اسمه على البحث أو الدِّراسة إسهام فكريّ معتبر في البحث أو الدِّراسة. ولا يعد مجرد التمويل، أو تجميع البيانات، معايير كافية لتثبيت حقّ أيّ شخص في التَّأليف.

6) يجب الإفصاح عن أيّ تعارض مصالح محتمل بين شخصيَّة الباحث وأيّة جهة علميَّة أو بحثيَّة يتّبعها الباحث، أو لها حقّ تبعيّ على البحث أو الدِّراسة. كما يتعيّن الإفصاح عن أيّة علاقة شخصيَّة أو ماليَّة بين الباحث وأي شخص أو منظمة من شأنها أن تؤثر على تفسير الباحث لنتائج بحثه أو دراسته، ويتمّ توثيق ذلك كتابة عند تقديم البحث أو الدِّراسة للنّشر بالمجلَّة.

7) يجب على الباحث ذكر كافة مصادر تمويل البحث أو الدِّراسة. وفي حالة وجود مصدر للتَّمويل، يتعيّن على الباحث الإشارة- بصورة تفصيليَّة- إلى اسم الوكالة المموَّلة أو الجهة المانحة.

8) تعد عملية تحكيم البحوث والدراسات التي تقدم للنشر في المجلة مرحلة رئيسية من مراحل النشر العلمي، ولذا يتعين على المحكمين- الداخليين والخارجيين- الالتزام بأخلاقيات النشر العلمي ومبادئه.

9) تتبع المجلة نهج التحكيم المخفي (المعمي) بحيث لا يعرف المحكم شخصية الباحث كما لا يعرف الباحث شخصية المحكم.

10) يتم إخضاع البحث لبرنامج فحص الاقتباس قبل إرساله للتحكيم، وفي حالة تعدي نسبة 25% من المرجع الواحد، أو تعدي نسبة 25% من المراجع ككل يتم إرجاع البحث للمؤلف.

11) يتعين على المحكم النأي بنفسه عن المصالح الشخصية كأن يستخدم معلومات حصل عليها من البحث الذي تم تحكيمه لمصلحته الشخصية.

12) يتعين على المحكم إخطار رئيس التحرير أو مدير التحرير، في حال عدم قبوله أو عدم استعداده لتحكيم البحث أو الدراسة، بذلك فور تسلمه، حتى يتسنى إرسال البحث أو الدراسة لمحكم آخر في الإطار الزمني المحدد.

13) يتعين على المحكم الالتزام بمعايير السرية المتعلقة بعملية التحكيم، والتعامل مع البحوث والدراسات محل التحكيم كوثائق سرية لا يجوز الكشف عنها خلال مرحلة التحكيم، أو مناقشتها مع الآخرين باستثناء رئيس التحرير أو مدير التحرير.

14) يتعين على المحكم التعبير عن رأيه العلمي فيما يرسل إليه من بحوث ودراسات لأغراض التحكيم بنزاهة وموضوعية ووضوح، مع تضمين تقرير التحكيم الحجج الداعمة لما ينتهي إليه بشأن صلاحية البحث أو الدراسة للنشر من عدمه.

15) يتعين على المحكم- الداخلي والخارجي- الالتزام بالوقت المخصص لعملية التحكيم.

البحوث والدراسات باللغة العربية

" تعبر المواد التي تنشر في المجلة عن آراء أصحابها ولا تعبر
بالضرورة عن رأي المجلة "

المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

(دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل الأدلة الرقمية)

الأستاذ الدكتور/ حسام نبيل الشنراقي

أستاذ علوم الشرطة - رئيس قسم إدارة الشرطة - أكاديمية شرطة دبي

المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي (دراسة تحليلية للأساليب الإجرامية وقواعد ضبط وتحليل الأدلة الرقمية)

الأستاذ الدكتور/ حسام نبيل الشنراقي
أستاذ علوم الشرطة – رئيس قسم إدارة الشرطة – أكاديمية شرطة دبي

المُلخَّص

يتناول البحث المواجهة الأمنية لجرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي، مع التركيز على الأساليب الإجرامية المعقدة التي يستخدمها المبتزون لاستغلال ضحاياهم. ويشمل الابتزاز الإلكتروني تهديد الضحية بنشر معلومات شخصية حساسة أو التشهير بها؛ للحصول على مكاسب مادية أو لا أخلاقية أو معنوية، وتبرز الدراسة تحديات عدة في مواجهة هذه الجرائم؛ مثل سهولة ارتكابها، وصعوبة تعقب الجناة، إلى جانب تطور الأدوات الرقمية المستخدمة في هذه الجريمة.

ويشير البحث إلى أهمية التحليل الجنائي الرقمي في مواجهة هذه الجرائم؛ حيث يعتمد على استرجاع الأدلة الرقمية، كالرسائل الإلكترونية والبيانات المخزنة، وفق أسس قانونية وتقنية تضمن قبولها أمام القضاء. كما يؤكد ضرورة تطوير كفاءات أمنية قادرة على التعامل مع الجرائم الرقمية، والتعاون بين الجهات الأمنية والقضائية لضبط الأدلة وتقديمها بطريقة مهنية.

يوفر البحث أيضًا حلولاً واستراتيجيات فعالة لمكافحة الابتزاز الإلكتروني؛ مثل تعزيز الوعي المجتمعي بمخاطر الإنترنت ووسائل التواصل الاجتماعي، وتطوير نظم الحماية الإلكترونية، بالإضافة إلى سن التشريعات القانونية التي تعاقب على هذه الجرائم، وتركز الدراسة على ضرورة تعزيز التعاون الدولي لمكافحة الابتزاز الإلكتروني العابر للحدود.

الكلمات المفتاحية: الابتزاز الإلكتروني – الجرائم السيبرانية – الحلول الأمنية – التحديات الأمنية – الإنترنت المظلم – التحقيقات الجنائية الرقمية – التشريعات السيبرانية – الوقاية من الجرائم الإلكترونية – التكنولوجيا الأمنية – حماية الخصوصية – التهديدات الإلكترونية – الابتزاز عبر وسائل التواصل الاجتماعي – التعاون الأمني الدولي.

ABSTRACT

Police Confrontation of Cyber Blackmail Crimes "Via Social Media" (An Analytical Study of Criminal Methods and Rules for seizing and Analyzing Digital Evidence)

Professor/ Hossam Nabil El-Shenraky
Professor of Police Sciences - Head of Police management Department - Dubai Police Academy

The research "Security Confrontation of Cyber Blackmail Crimes: Challenges and Solutions" deals with a comprehensive study of cyber blackmail crimes via social media, focusing on the complex criminal methods used by blackmailers to exploit their victims. Cyber blackmail includes threatening the victim with publishing sensitive personal information or defaming them in order to obtain material, sexual or moral gains. The study highlights several challenges in confronting these crimes, such as the ease of committing them and the difficulty of tracking down the perpetrators, in addition to the development of digital tools used in the crime. The study indicates the importance of digital forensic analysis in confronting these crimes, as it relies on retrieving digital evidence such as emails and stored data, according to legal and technical foundations that ensure their acceptance before the judiciary. It also emphasizes the need to develop security competencies capable of dealing with digital crimes, and cooperation between security and judicial authorities to seize evidence and present it in a professional manner. The study also provides effective solutions and strategies to combat cyber blackmail, such as enhancing community awareness of the dangers of the Internet and social media, developing electronic protection systems, in addition to enacting legal legislation that punishes these crimes. The study focuses on the need to enhance international cooperation to combat cross-border cyber blackmail.

Keywords: Cyber extortion - Cybercrime - Security solutions - Security challenges - Dark web - Digital forensics - Cyber legislation - Cybercrime prevention - Security technology - Privacy protection - Cyber threats - Social media extortion - International security cooperation

التمهيد:

في عصر يتسم بالتكنولوجيا الرقمية والاتصالات الفورية، أصبح الابتزاز الإلكتروني ظاهرة متزايدة الانتشار والخطورة، وقد أصبح هذا النوع من الجريمة الإلكترونية يمثل تحديًا كبيرًا للأفراد والمؤسسات على حد سواء؛ حيث يستخدم المجرمون التكنولوجيا للضغط على ضحاياهم بهدف تحقيق مكاسب مالية أو شخصية.

ويتضمن الابتزاز الإلكتروني مجموعة واسعة من الأنشطة الضارة؛ مثل التهديد بنشر معلومات خاصة، أو التشهير عبر الإنترنت، أو التهديد بإلحاق الضرر بالأفراد أو المؤسسات إذا لم يتم تلبية مطالب الشخص المبتز، كما يتميز هذا النوع من الجرائم بسهولة التنفيذ وصعوبة تتبع المجرمين، مما يجعله تحديًا كبيرًا أمام أنظمة القانون والأمن الإلكتروني.

وتعد جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي من أخطر الجرائم الإلكترونية في العصر الحديث؛ حيث تستهدف هذه الجرائم الأفراد والمؤسسات عبر استغلال الثغرات الأمنية واستدراج الضحايا بطرق وأساليب إجرامية معقدة. وإن تزايد الاعتماد على التكنولوجيا وانتشار وسائل التواصل الاجتماعي أدى إلى ظهور أنماط جديدة من الجرائم، تتطلب مواجهة أمنية تعتمد على التحليل الدقيق للأساليب الإجرامية، وضبط الأدلة الرقمية وتحليلها بطرق احترافية، لذلك فإن دراسة تلك الجرائم وتحليل أساليبها يمثل ضرورة أمنية مُلِحَّة؛ لفهم طبيعة التهديدات وكيفية التعامل معها بشكل فعال.

كما أن الأساليب الإجرامية في جرائم الابتزاز الإلكتروني متعددة؛ إذ تشمل الاستدراج العاطفي، والتلاعب النفسي، والاحتيال عن طريق خلق هويات وهمية، ولجوء المجرمين إلى استخدام برامج تجسس وتقنيات متطورة لاختراق الخصوصية، مما يعقد عملية جمع الأدلة وضبط الجناة أمام هذه التحديات، لذلك تأتي أهمية التحليل الجنائي الرقمي، الذي يعتمد على تتبع آثار الجريمة في الفضاء السيبراني، واستخدام أدوات متقدمة لاستعادة وتحليل البيانات من الأجهزة والشبكات التي تم استهدافها، ويعتمد نجاح هذه التحليلات على دقة وكفاءة الأدوات المستخدمة، وكذلك على كفاءة الكوادر المؤهلة في هذا المجال.

في هذا السياق، تبرز قواعد ضبط وتحليل الأدلة الرقمية كعنصر أساسي في المواجهة الأمنية لجرائم الابتزاز الإلكتروني، الأدلة التي تشمل الرسائل الرقمية، والصور، والمعلومات المخزنة على الأجهزة الإلكترونية، التي تتطلب معالجة دقيقة وفقًا لمعايير قانونية وتقنية صارمة تضمن قبولها أمام القضاء. ويعتمد ضبط هذه الأدلة على استخدام تقنيات الاسترجاع الرقمي دون المساس بسلامة البيانات، مما يشكل تحديًا في الحفاظ على التسلسل الزمني للأحداث وكشف العلاقات بين الأطراف المتورطة. كما أن التحليل الجنائي الرقمي يجب أن يتم بصورة تحافظ على حقوق الأفراد وخصوصياتهم، مع الأخذ في الاعتبار الجوانب الأخلاقية والقانونية.

وتؤكد هذه الدراسة التحليلية أن المواجهة الأمنية الفعالة لجرائم الابتزاز الإلكتروني تتطلب نهجًا متكاملاً يشمل فهم الأساليب الإجرامية المتجددة، وضبط الأدلة الرقمية بأساليب احترافية تضمن صحتها أمام القضاء، وكذلك فإن التعاون بين الأجهزة الأمنية والجهات القضائية، بالإضافة إلى تطوير قدرات التحليل الجنائي الرقمي، هو السبيل الأنجح لمكافحة هذا النوع من الجرائم. وفي ظل التطور السريع في تقنيات الجريمة الإلكترونية، يصبح من الضروري الاستثمار المستمر في تدريب الكوادر الأمنية، وتطوير أدوات التحليل الرقمي، ورفع مستوى الوعي المجتمعي بطرق الوقاية من هذه الجرائم.

فالانفتاح التقني وما صاحبه من قفزة نوعية في الاتصالات بشكل عام وفي مجال الإنترنت بشكل خاص قد أوجد عدة مظاهر سلبية نجمت عن سوء استخدام الوسائل الإلكترونية التي من المفروض أنها وجدت حتى تخدم بني البشر لا أن تكون سببًا في تعاستهم[1].

أهمية الدراسة:

تعد جرائم الابتزاز الإلكتروني من الجرائم متعددة الأبعاد وشديدة الخطورة، وذلك لما تمثله من قهر للضحية يمارسه الجاني عليها حتى يحصل على مبتغاة، كما أنه قد يؤدي إلى آثار شديدة الخطورة على الأمن؛ حيث قد يؤدي بالضحية إلى الانتحار للتخلص من العار الذي يلحق بها بسبب فضح أسرارها أو هتك ستر خصوصياتها، كما أنها من الجرائم التي تحتاج إلى استراتيجية خاصة في التعامل معها؛ لما تتضمنه من خوف شديد لدى الضحية، وهو ما يتطلب دراسة مستفيضة يمكن من خلالها التوصل إلى آلية مُثلى تحقق مواجهة أمنية مستنيرة وقادرة على فهم التحديات وكيفية مكافحة هذه الجريمة الخطيرة.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في إيجاد آلية متعددة المحاور يمكن من خلالها تحقيق مواجهة أمنية متكاملة لجرائم الابتزاز الإلكتروني بصورها المختلفة وأنماطها المتعددة، وهو ما يحتاج إلى دراسة متكاملة الجوانب يمكن من خلالها فهم الطبيعة شديدة الخطورة للجريمة؛ من خلال فهم وتحليل الأنماط المختلفة للجريمة، وفهم طبيعة الجناة والأدوات التي يستخدمونها للإيقاع بضحاياهم، واستراتيجية الجناة في إجبار ضحاياهم على الاستجابة لهم، وفهم طبيعة الأدلة الرقمية المتخلفة عن الجريمة، وكيفية حفظها وتحصيلها وفقًا للأسس الصحيحة، وتحليلها وصولاً لتحديد شخصية الجناة وإثبات الجريمة عليهم.

(1) د/ سعيد زيوش - ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية – مجلة العلوم الاجتماعية – يناير -2017 العدد 22 – 2017م – ص70ص73

أهداف الدراسة:

تهدف الدراسة إلى تحقيق عدة أهداف تتمثل في:

1. دراسة وتحليل طبيعة جريمة الابتزاز الإلكتروني، وأساليب ارتكابها، وخصائصها، وأنماطها، وسمات مرتكبيها.
2. تحديد وتحليل التحديات الأمنية المرتبطة بجرائم الابتزاز الإلكتروني، وإيجاد حلول لها.
3. فهم وتحليل الطبيعة الخاصة للأدلة الرقمية، وأساليب حفظها وفحصها وتحليلها.
4. إيجاد حلول واستراتيجيات لمكافحة الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

تساؤلات الدراسة:

1. ما المقصود بجرائم الابتزاز الإلكتروني؟
2. ما أنماط الابتزاز الإلكتروني؟
3. ما خصائص ودوافع جريمة الابتزاز الإلكتروني؟
4. كيف نظم القانون القطري والقانون الإماراتي تجريم الابتزاز الإلكتروني؟
5. ما القواعد الإجرائية للتعامل مع الأدلة الرقمية في القانون القطري؟
6. ما القواعد الفنية للتعامل مع الأدلة الرقمية؟

منهج الدراسة:

نتبع في هذه الدراسة المنهج الوصفي التحليلي القائم على وصف جريمة الابتزاز الإلكتروني وأسبابها كافة والآثار المترتبة عليها، وتوضيح أنماطها المختلفة وصولاً إلى فهم الأساليب الإجرامية الحالية كافة، وتحليل كيفية ارتكاب الجاني للجريمة، وفهم دوافعه وكيفية وقوع الضحية في الجريمة، والوصول من خلال التحليل إلى آلية مُثلى للوقاية من الجريمة، وكذلك كيفية التعامل مع الجريمة بأبعادها المختلفة لإقناع الضحايا بالإبلاغ في ظل آلية للحفاظ على سمعة الضحية وسرية المعلومات الخاصة بها، ثم تحقيق مواجهة أمنية فاعلة للجريمة، وضبط الجناة للحد من الجريمة.

نطاق الدراسة:

النطاق الموضوعي: تتضمن الدراسة فهم وتحليل أساليب جريمة الابتزاز الإلكتروني، وسمات مرتكبيها، وكيفية استدراج الضحايا عبر مواقع التواصل الاجتماعي، والإجراءات التي يمكن أن يقو م بها رجال البحث الجنائي لضبط الأدلة الرقمية على الجريمة، وتشريحها للوصول لشخص مرتكبها، وأساليب التحري عن الجريمة.

أدوات الدراسة:

يستخدم الباحث في الدراسة المراجع العلمية المختلفة والدراسات التي أجريت في هذه الجريمة، وكذلك التجارب المختلفة في المكافحة، ودراسات الحالة، وصولاً إلى أفضل التطبيقات والممارسات في مجال التحري عن جرائم الابتزاز الإلكتروني وضبط الأدلة عليها وضبط مرتكبيها.

الدراسات السابقة:

1- أطروحة ماجستير بعنوان: "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي (الفيسبوك نموذجًا)". وهي دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال بجامعة قاصدي مرباح – تخصص تكنولوجيا الاتصال الجديدة – الجزائر، مقدمة من سمان جويدة، وإيمان مردف 2017م. وقد تناولت الدراسة أهمية منصة (FaceBook) في التواصل الاجتماعي، ومخاطر استخدامه في استدراج الفتيات لابتزازهم إلكترونيًا، ووضحت دوافع واحتياجات الفتيات لاستخدام هذه المنصة؛ كإشباع الحاجة العاطفية، وما يسببه من وقوعهنَّ ضحايا للابتزاز، وكيف يمكن استخدامه بشكل صحيح لعدم الوقوع ضحية للجريمة، واعتمدت الدراسة في توضيح ذلك على إجراء مسح تحليلي لمجموعة فتيات في كلية تكنولوجيا الإعلام في الجامعة من خلال الاستبانة، وتوصلت الدراسة إلى أن السبب الأساسي لوقوع الفتيات ضحايا للجريمة هو عدم كفاية الوعي لديهنَّ بمخاطر هذه المواقع، والتهاون في تبادل البيانات الشخصية عبرها مع غرباء، وعدم اتباع القواعد الصحيحة في هذا الشأن.

2- دراسة محمد حسن مكاوي بعنوان: "الابتزاز الإلكتروني بين التهديد والحماية (دراسة في التشريعات المصرية والأمريكية – Journal of Law and Emerging Technologies issued by the Faculty of Law at the British University in Egypt, Volume 02, Issue 02 October 2022,)

قدَّمت هذه الدراسة تحليلاً شاملاً لظاهرة الابتزاز والتهديد الإلكتروني، وتعريف الابتزاز الإلكتروني وأنواعه وآثاره المجتمعية، وعقدت مقارنة بين القوانين المعمول بها لهذه الجريمة في التشريعين المصري والأمريكي، مع عرض أحدث القضايا الخاصة بتلك الجريمة، وموقف الأحكام القضائية منها، بالإضافة إلى البيانات الإحصائية التي توضح مدى اتساع الظاهرة في المجتمعين المصري والأمريكي. كما أظهرت الدراسة كيف أدى التحول الرقمي إلى زيادة انتهاك الخصوصية عبر الإنترنت، وأظهرت الفجوة بين التشريعات المصرية والتطور الهائل في تكنولوجيا المعلومات والتحول الرقمي، مما أكد حتمية وضرورة سن التشريعات لمواجهة أنواع الجرائم المستحدثة بأشكالها المختلفة وبطرق ارتكابها المتنوعة. وقد حاول الباحث أن يضع بعض الحلول للعقبات الإجرائية التي تؤثر على تطبيق العدالة السريعة والردع العام.

خطة الدراسة:

المبحث الأول: ماهية جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

- **المطلب الأول: التعريف بجريمة الابتزاز الإلكتروني.**
  - الفرع الأول: مفهوم جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: الابتزاز الإلكتروني في الفقه.
  - الفرع الثالث: الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م والقانون الإماراتي رقم 34 لسنة 2021م.
- **المطلب الثاني: خصائص ودوافع وأنماط ومحاور جريمة الابتزاز الإلكتروني.**
  - الفرع الأول: خصائص جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: دوافع جريمة الابتزاز الإلكتروني.
  - الفرع الثالث: أنماط ومحاور الابتزاز عبر مواقع التواصل الاجتماعي.

المبحث الثاني: إجراءات التحقيق في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

- **المطلب الأول: الإطار الإجرائي القانوني لجريمة الابتزاز الإلكتروني في التشريع القطري.**
  - الفرع الأول: الشكوى في جريمة الابتزاز الإلكتروني.
  - الفرع الثاني: إجراءات ضبط الأدلة الإلكترونية في جريمة الابتزاز الإلكتروني.
  - الفرع الثالث: شروط صحة الدليل الإلكتروني في جريمة الابتزاز الإلكتروني أمام القضاء الجنائي.
- **المطلب الثاني: القواعد الفنية لجمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.**
  - الفرع الأول: مرحلة الإعداد وجمع الأدلة من مواقع التواصل الاجتماعي.
  - الفرع الثاني: توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي.
  - الفرع الثالث: تحليل الأدلة في جرائم الابتزاز الإلكتروني.

مصطلحات الدراسة:

الابتزاز الإلكتروني، الجريمة الإلكترونية، الأدلة الرقمية، التحليل الجنائي الرقمي، التشريح الرقمي للأدلة، تحريز الأدلة الرقمية، الجرائم المستحدثة، التحقيق الجنائي الرقمي.

المبحث الأول
ماهية جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

التمهيد:

تعد جريمة الابتزاز الإلكتروني من الجرائم المستحدثة التي ظهرت مع ظهور التقنيات الحديثة في نقل وتبادل الوسائط الإلكترونية وتطور وسائل التواصل الاجتماعي، وتعاظم تأثيرها على المستخدمين، وسوف نتناول بالدراسة في هذا المبحث التعريف بالابتزاز الإلكتروني وخصائص الجريمة وسمات الجناة في مطلبين: **المطلب الأول:** التعريف بجريمة الابتزاز الإلكتروني، **والمطلب الثاني:** خصائص ودوافع جريمة الابتزاز الإلكتروني.

المطلب الأول: التعريف بجريمة الابتزاز الإلكتروني

الفرع الأول: مفهوم جريمة الابتزاز الإلكتروني

تم تعريف الابتزاز الإلكتروني في القانون القطري كأحد أشكال الجرائم الإلكترونية التي تمثل اعتداءً على حرية الضحية وملكيتها أو خصوصيتها عبر استخدام وسائل تقنية المعلومات مثل الشبكة المعلوماتية، وذلك بهدف تحقيق مكاسب غير مشروعة أو إجبار الضحية على القيام بأفعال لا ترغب بها. كما أن الابتزاز الإلكتروني قد يرتبط بتهديد الضحية بفضح معلومات خاصة أو حساسة، وفي بعض الأحيان قد يشمل تهديدًا بالإضرار بالسمعة أو بالأسرة.

وقد أشار المشرع القطري إلى جريمة الابتزاز الإلكتروني في القانون رقم 14 لسنة 2014 بشأن مكافحة الجرائم الإلكترونية؛ حيث جاء في المادة 9 من هذا القانون أنه: "يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات أو بغرامة لا تزيد على مئة ألف ريال قطري، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات لابتزاز أو تهديد شخص لحمله على القيام بعمل أو الامتناع عنه". وتعتبر هذه المادة أساسًا قانونيًا لتعريف الابتزاز الإلكتروني في قطر؛ حيث يرتكز التعريف على استخدام التهديد بوسائل تقنية المعلومات لتحقيق أهداف غير مشروعة، وقد تبنى المشرع القطري تعريفًا واسعًا لجريمة الابتزاز الإلكتروني؛ إذ لم يحدد بشكل ضيق مضمون التهديد، بل اكتفى بذكر أن التهديد يكون لتحقيق هدف محدد، مثل "حمل الضحية على القيام بعمل أو الامتناع عنه". وبهذا ينظر المشرع إلى الابتزاز الإلكتروني على أنه جريمة متكاملة الأركان إذا تحقق فيها فعل التهديد بواسطة الشبكة المعلوماتية.

ويلاحظ أن القانون رقم 14 لسنة 2014م لم يوضح تعريف جريمة الابتزاز بشكلٍ كافٍ، بينما تناولت المادة 325 من قانون العقوبات القطري جريمة التهديد؛ حيث عرفها المشرع باعتبارها تهديدًا مقترنًا بطلب يلحق ضررًا بالشخص نفسه أو بسمعته أو بماله أو بسمعة شخص يهمه أمره، وذلك لتحقيق مكاسب مادية أو معنوية. وتتنوع الوسائل المستخدمة لتهديد المجني عليه؛ سواء كانت مكتوبة أو شفهية أو باستخدام وسائل أخرى، بشرط أن توحي هذه الأفعال بالعزم على إلحاق الأذى بالشخص أو من يهمه أمره، وعلى ذلك فقد تضمنت المادة 325 تحديد شكل التهديد؛ حيث يمكن أن يكون التهديد مكتوبًا أو شفهيًا أو بأي وسيلة توحي بجدية العزم على إيقاع الضرر، ويستهدف التأثير على إرادة المجني عليه لتحقيق طلب معين من قبل الجاني، وتحديد الغاية من التهديد وهي أن ينصب التهديد على تحقيق غاية معينة، مثل حمل المجني عليه على القيام بعمل ما أو الامتناع عنه؛ حيث تتضح جريمة الابتزاز في هذه الحالة من خلال ربط التهديد بهدف محدد يطلبه الجاني.[2]

كما تعرف جريمة الابتزاز الإلكتروني بأنها: "استخدام التكنولوجيا الرقمية مثل الإنترنت أو الهواتف الذكية لتهديد الأفراد أو المؤسسات بهدف الحصول على المال أو الخدمات أو لغرض آخر بالقوة أو التهديد. ويتضمن الابتزاز الإلكتروني إرسال رسائل تهديدية أو التشهير بالشخص أو نشر معلومات خاصة بهدف إجبار الضحية على القيام بشيء معين؛ مثل دفع مبلغ مالي أو تقديم خدمات أخرى. على أن هذه الأفعال تعتبر غير قانونية وتعرض مرتكبها للمساءلة القانونية بموجب القوانين المحلية والدولية المعمول بها".

إن جريمة الابتزاز الإلكتروني هي شكل من أشكال الجريمة الإلكترونية التي تتمثل في استخدام وسائل الاتصال الإلكتروني؛ مثل الرسائل النصية، والبريد الإلكتروني، والمنصات الاجتماعية، والتطبيقات الرقمية، لتهديد الأفراد أو المؤسسات بهدف الحصول على مال أو خدمات أو لأغراض أخرى بالقوة أو التهديد[3].

وتعتبر جريمة الابتزاز الإلكتروني تطورًا للابتزاز التقليدي؛ حيث تستخدم التكنولوجيا لتوسيع نطاق الضغط على الضحية وتكوين حدود أقل وضوحًا بالنسبة للمرتكب، فعلى سبيل المثال يمكن للمعتدين استخدام الصور أو الفيديوهات الخاصة بالضحية ونشرها عبر الإنترنت كوسيلة للابتزاز المالي أو العاطفي.

(2) جاسم ناصر جاسم المسلماني – التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري – رسالة مقدمة للحصول على درجة الماجستير في القانون العام – كلية القانون – جامعة قطر – يناير 2023م – ص7ص9

(3) Martinez, M., & Anderson, C, "Cyber Extortion: An Emerging Internet-Based Crime", Journal of Cybersecurity, 2021, pp: 126129-

وجريمة الابتزاز الإلكتروني هي استخدام الإلكترونيات وتكنولوجيا المعلومات لتهديد الأفراد أو المؤسسات بأن ينشروا أو يعرضوا معلومات محرجة أو خاصة عبر الإنترنت أو الوسائل الرقمية الأخرى مقابل متطلبات مالية أو أخرى[4].

ويعرف الابتزاز الإلكتروني أيضًا بأنه الأفعال التي تتضمن إساءة استخدام شبكة المعلومات لتحقيق غرض غير مشروع يختلف بحسب ظروف كل فعل وبحسب مرتكب الفعل، ويهدف إلى تحقيق أهداف مالية أو لا أخلاقية أو معنوية.

كما يمكن تحديد الابتزاز الإلكتروني على أنه الأفعال التي يستخدم مرتكبها التقنيات المتقدمة عبر الإنترنت والبرمجيات التي تمكنه من محو آثار الجريمة عقب ارتكابها وصولاً لتحقيق غاياته؛ حيث تختلف الغايات باختلاف مرتكبي الجريمة وباختلاف المؤثرات التي تؤثر عليهم.

ويرى الباحث تعريف الابتزاز الإلكتروني على أنه: "استخدام التكنولوجيا الرقمية؛ مثل الإنترنت والهواتف الذكية، لتهديد الأفراد أو المؤسسات بهدف إجبارهم على تقديم مال أو خدمات أو لتحقيق أهداف أخرى غير مشروعة. ويتم ذلك من خلال التهديد بنشر معلومات خاصة أو محرجة، أو إرسال رسائل تهديدية، ويستغل مرتكب الجريمة وسائل الاتصال الإلكتروني مثل البريد الإلكتروني ومنصات التواصل الاجتماعي لتحقيق غاياته. وتختلف هذه الغايات وفقًا لظروف الجريمة، وتشمل الأهداف المالية أو غير الأخلاقية أو المعنوية، ويستخدم المبتزون تقنيات متقدمة لإخفاء آثار الجريمة" .

الفرع الثاني: الابتزاز الإلكتروني في الفقه

عرَّف بعض الفقهاء الابتزاز بأنه إكراه يمارسه شخص على إرادة آخر ليجبره على فعل جريمة، وعرفه آخرون بأنه: "فعل يرتكبه شخص بتهديد آخر بالقول أو بالكتابة، باستخدام وسائل للتأثير على نفسية الضحية لتخويفه، أو لإزعاجه من خطر لم يحدث بعد، يترتب عليه إلحاق الضرر بماله، أو بشخصه، أو بشخص آخر ذي صلة بالمجني عليه"، وعُرِّف أيضًا بأنه: "تهديد شخص بفضح أمره ما لم يستجب لطلبات الجاني غير المشروعة التي تمس الشرف، أو تتعلق بحرمة الحياة الخاصة للضحية" .

(4) Kasmani, M. F., Ismail, R., Sulong, R. S., & Mahamod, Z. (2018). Cyber blackmailer: Modus operandi and preventive measures. International Journal of Cyber Criminology, 12(2), 334345-

كما عرف بأنه: "الحصول على مستندات أو صور أو معلومات عن الضحية باستخدام وسائل إلكترونية، أو التهديد بالتشهير بمعلومات ووثائق سرية باستخدام التقنيات الإلكترونية لتحقيق أهداف المبتز".[5]

وعرف بأنه: "القيام بالمحاولة للحصول على منفعة مادية أو معنوية من إنسان طبيعي أو شخص معنوي بالإجبار عن طريق تهديده بفضح سره أو استخدام القوة مقابل ضعف الضحية المؤقت أو الدائم"، وعرفه آخرون بأنه سلب إرادة وحرية شخص عن طريق إيذائه بدنيًا أو نفسيًا باستخدام أساليب لا أخلاقية.

كما يعرفه بعض الفقهاء بأنه سلوك غير مشروع يقع باستخدام المواقع الإلكترونية كمنصة (FaceBook)، أو الأجهزة الإلكترونية كالهواتف الذكية وغيرها، وهو أيضًا: "تهديد الجاني للمجني عليه عقب الحصول على معلومات حساسة له كمقاطع الصوت، أو الصور أو المقاطع المصورة أو المحادثات المكتوبة إلكترونيًا لتحقيق منفعة مادية أو معنوية"،[6] كما عرف بأنه: "الحصول على أسرار أو صور، أو مقاطع مصورة لشخص واستخدامها في إجباره على دفع مبالغ مالية للجاني أو إتيان أفعال يجرمها القانون أو تنافي الأخلاق، كتهديد الإناث بنشر صور خاصة لهن على مواقع الإنترنت، أو إبلاغ أقاربهن في حال لم يستجبن لمطالب المبتز".

يتبين من التعريفات السابقة للابتزاز التقليدي أو الإلكتروني أنه وسيلة لإجبار الضحايا أو تهديدهم بواسطة المبتز لتنفيذ إرادته، والابتزاز مرتبط بالتهديد، فلا يمكن أن تتحقق إرادة المبتز دونه.[7]

وعلى ذلك فجريمة الابتزاز الإلكتروني يقوم فيها الجاني باستخدام مهاراته التقنية وبرمجيات متطورة لاختراق المواقع والبيانات المخزنة على الوسائط المتصلة بالإنترنت أو بالشبكات المحلية والدولية، ويمكنه بواسطتها التوصل لبيانات حساسة؛ سواء بواسطة أشخاص أو مؤسسات لاستخدامها للحصول بالتهديد على غاياته الشخصية، أو تحقيق غايات آخرين.

(5) ام د / احمد سبتي احمد، اد/ محمد نعمان عبد النبي – الابتزاز الإلكتروني واثرة في تهديد المجتمع" دراسة فقهية معاصرة " - كانون الثاني 25, 2022 - مجلة جامعة تكريت للعلوم الانسانية المجلد -1 الجزء الاول عدد خاص بالمؤتمر لعام 2022 العدد 29 – ص55ص57 - https://jtuh.org/index.php/jtuh/article/view/1740

(6) شريفة محمد السويدي – د/ زيزيت مصطفي نوفل – اسباب الابتزاز الإلكتروني والاثار الاجتماعية والنفسية المرتبطة به " دراسة كيفية" – مجلة الآداب – العدد 146 – ايلول 2023م – ص616ص618 – Dio: https: //doi.org/10.31973/ 3583/aj.v1i146.4008https://aladabj.uobaghdad.edu.iq/index.php/aladabjournal/article/view/4008

(7) الباحث. باقر غازي حنون، أ.د. حسن حماد حميد - جريمة الابتزاز الإلكتروني (دراسة مقارنة(- مجلة دراسات البصرة - السنة السادسة عشرة / ملحق العدد (42) كانون الأول 2021 – ص53ص54

ويهدف المبتز غالبًا للحصول على مال من الضحية أو علاقة غير مشروعة، أو تلبية طلب طرف آخر تحقيقًا لمنفعة شخصية أو مكاسب مالية يحصل عليها عند تنفيذ المطلوب، كإفشاء أسرار شركة لمنافسيها، أو الحصول على معلومات تمس الأمن القومي لبيعها للأعداء، أو بيع بيانات مؤسسة إذا لم يتم الاستجابة لطلباته، كأن يطلب توظيفه فيها.[8]

ويرى الباحث تعريف الابتزاز الإلكتروني وفقًا لما انتهى إليه رأي الفقه على النحو التالي: "الابتزاز الإلكتروني هو استغلال الجاني للتقنيات الرقمية والبرمجيات المتطورة لاختراق البيانات أو الحصول على معلومات حساسة تخص الضحية؛ سواء كانت شخصًا طبيعيًا أو معنويًا، ثم استخدام تلك المعلومات لتهديد الضحية بنشرها أو استخدامها لتحقيق مطالب غير مشروعة. هذه المطالب قد تكون مالية، أو معنوية، أو غير أخلاقية، وغالبًا ما تكون مدفوعة بمصلحة شخصية أو لتحقيق مكاسب مالية، أو حتى خدمة لأطراف أخرى. ويتم ذلك التهديد عبر وسائل الاتصال الإلكتروني مثل البريد الإلكتروني، أو الرسائل النصية، أو منصات التواصل الاجتماعي، ويعتمد المبتز على التأثير النفسي والتخويف لإجبار الضحية على الامتثال".

الفرع الثالث: الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م والقانون الإماراتي رقم 34 لسنة 2021م

أولًا: أركان جريمة الابتزاز الإلكتروني في القانون القطري رقم 14 لسنة 2014م:

كي تتحقق جريمة الابتزاز الإلكتروني، يجب أن تتوفر فيها أركان أساسية تشمل:

1. الركن المادي: ويتمثل في فعل التهديد المقترن بطلب معين من الضحية، ويشمل ثلاثة عناصر:

أ- فعل التهديد: هو السلوك الذي يقوم به الجاني لإيقاع الخوف أو الرعب في نفس الضحية، وقد يتم التهديد بطرق مختلفة؛ مثل إرسال رسائل تهديدية عبر البريد الإلكتروني أو الرسائل النصية، أو نشر معلومات خاصة بالضحية على وسائل التواصل الاجتماعي. ويشترط أن يكون التهديد جديًا وليس على سبيل المزاح، وأن يكون قادرًا على التأثير على إرادة المجني عليه.

(8) (Kshetri, N. (2010). "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives." Springer, 2010, pp: 3537-, http: //ndl.ethernet.edu.et/bitstream/12345678950/1/26704/.pdf

ب- الغاية من التهديد: يكون الهدف من التهديد هو إجبار الضحية على القيام بفعل محدد أو الامتناع عنه. والغاية قد تكون تحقيق منفعة مادية مثل المال، أو منفعة معنوية مثل الحصول على معلومات سرية. ويجب أن يكون التهديد مرتبطًا بغاية معينة لاعتبار الابتزاز الإلكتروني مكتمل الأركان.

ج- وسيلة التهديد: يحدد القانون القطري أن تكون وسيلة التهديد عبر تقنية المعلومات أو الشبكة المعلوماتية؛ أي أن الجريمة لا تقع بدون استخدام الوسائل الإلكترونية، مثل البريد الإلكتروني أو وسائل التواصل الاجتماعي.

2. الركن المعنوي: يتطلب الركن المعنوي في جريمة الابتزاز الإلكتروني وجود نية جنائية؛ أي أن الجاني لديه نية واضحة في إلحاق الضرر بالضحية، وتحقيق مكاسب غير مشروعة من وراء ذلك، ويجب أن يكون القصد الجنائي متوفرًا، بحيث يكون الجاني مدركًا وواعيًا لأفعاله ونتائجها، ويعتمد الركن المعنوي على عنصرين:

أ- القصد العام: ويشمل علم الجاني بأن فعله غير قانوني وأنه يستخدم وسيلة التهديد لإلحاق الخوف أو الضرر بالضحية.

ب- القصد الخاص: وهو رغبة الجاني في تحقيق هدف معين من جريمته، مثل الحصول على المال أو المعلومات أو أي منفعة أخرى.

ووفقًا للمادة 9 من القانون القطري لمكافحة الجرائم الإلكترونية (القانون رقم 14 لسنة 2014)، فإن العقوبة المقررة لجريمة الابتزاز الإلكتروني هي الحبس لمدة تصل إلى ثلاث سنوات، وغرامة تصل إلى مائة ألف ريال قطري. وقد يتم الحكم بإحدى هاتين العقوبتين أو بكلتيهما معًا حسب ظروف الجريمة وشدتها.

وتتنوع آراء الفقهاء وشروحاتهم حول المادة 9 من القانون القطري رقم 14 لسنة 2014 بشأن الابتزاز الإلكتروني، كما تعتمد على تفسير مبادئ الشريعة الإسلامية والقوانين الحديثة في مواجهة الجرائم الإلكترونية؛ حيث يتفق الفقهاء على أن الابتزاز الإلكتروني يمثل انتهاكًا للشريعة؛ إذ يقوم على الغش والتهديد والاستيلاء على حقوق الآخرين بغير وجه حق، وهذا العمل يعتبر محرمًا شرعًا لأنه يتضمن الإكراه والضرر، وهو ما حرمه الإسلام صراحة، ويشير العديد من الفقهاء إلى أن الابتزاز الإلكتروني يعد امتدادًا لمفهوم "الابتزاز" في الشريعة، ويشبهه كثيرًا بـ "التهديد" (الوعيد) للحصول على منفعة غير مشروعة. ووفقًا للشريعة يعتبر أي شكل من أشكال الاستغلال أو التهديد للحصول على مكاسب مادية أو

معنوية أمرًا محرمًا، كما يشدد الفقهاء على أن العقوبات المقررة في القانون تتماشى مع مقاصد الشريعة في تحقيق الردع وحماية الناس. ومن منظور إسلامي فإن الشريعة تجيز وضع قوانين حديثة تعاقب على الجرائم التي تهدد أمن الأفراد والمجتمع، بما في ذلك الجرائم الإلكترونية، كما يشير الفقهاء إلى أن الشريعة تحث على إزالة الضرر، فالابتزاز الإلكتروني يسبب ضررًا نفسيًا وماديًا للضحايا. وبالتالي فإن تجريم هذا الفعل يتفق مع مبدأ "لا ضرر ولا ضرار" في الإسلام، مما يعطي القوانين الوطنية الحق في فرض عقوبات لحماية الأفراد، ويوضح بعض الفقهاء أن الابتزاز الإلكتروني يمس العرض والكرامة، وهي أمور يجب حمايتها شرعًا، كما أن استخدام وسائل التهديد والإكراه على الإنترنت لمساس سمعة أو شرف شخص معين يعتبر من المحرمات، لذا فمن الضروري وجود قانون يعاقب على مثل هذه الجرائم لحماية خصوصيات الأفراد، ويرى الفقهاء أن سن قانون يحمي الناس من الابتزاز الإلكتروني يصب في مصلحة المجتمع، ويعزز الأمان والثقة في وسائل التواصل الإلكتروني. وإن الشريعة الإسلامية تبيح التشريعات الوضعية، مثل هذا القانون، إذا كانت تهدف إلى درء المفاسد وجلب المصالح.

بشكل عام، يثني الفقهاء على جهود الدولة في سن مثل هذا القانون وفرض عقوبات صارمة على جريمة الابتزاز الإلكتروني، ويعتبرونها خطوة ضرورية لحماية الأفراد والمجتمع من أضرار هذا النوع من الجرائم المتطورة التي ظهرت مع انتشار التكنولوجيا.[9]

وقد ركزت محكمة التمييز القطرية في حكم لها في جريمة الابتزاز الإلكتروني على أهمية توفر القصد الجنائي لدى المتهم في مثل هذه القضايا، فقد أكدت أن القصد الجنائي – كعنصر من عناصر الجريمة– يجب استخلاصه من الظروف المحيطة والأدلة المتوفرة، وأنه يدخل ضمن السلطة التقديرية لقاضي الموضوع. وبمعنى آخر، تُقِرُّ المحكمة بأن القصد الجنائي هو نية الجاني في تنفيذ التهديد لتحقيق مصلحة شخصية، ويتم استنتاجه من أفعال الجاني وسلوكه وظروف القضية، كما أكدت المحكمة أن التهديد عبر الوسائل الإلكترونية يعتبر جريمة مكتملة إذا كان التهديد جديًا ومصحوبًا بطلب من الضحية؛ مثل إجبارها على دفع المال أو القيام بأمر معين تحت طائلة تهديد بإيذاء سمعتها أو مصالحها.[10]

ثانيًا: الابتزاز الإلكتروني في القانون الإماراتي رقم 34 لسنة 2021م:

تعد جريمة الابتزاز الإلكتروني من الجرائم الخطيرة التي تهدد المجتمعات، ويعد التهديد والابتزاز سبب تجريمه، فالابتزاز الإلكتروني يمكن تعريفه بأنه: "تهديد شخص لحمله على

(9) جاسم ناصر جاسم المسلماني – التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري - مرجع سابق – ص21ص25

(10) الطعن 63 لسنة 2017 تمييز جنائي

القيام بفعل أو الامتناع عن فعل، ولو كان القيام بالفعل أو الامتناع عنه مشروعًا، وذلك باستخدام نظم المعلومات".

والابتزاز الإلكتروني له عدة أنواع، منها الابتزاز المادي، وهو تهديد الجاني للمجني عليه بالصور والمقاطع المرئية والمستندات على سبيل المثال، ومنها الابتزاز المعنوي، وهو تهديد الضحية بوسائل معنوية كاستخدام العبارات الشديدة لتهديده وتوعده بفضح أمره حتى يعتقد بجدية الجاني في تهديده، وتتنوع أهداف الجناة ما بين مادية و غير أخلاقية ونفعية.

وتتضمن المادة 42 من القانون الإماراتي أن كل من قام بابتزاز أو تهديد آخر لإجباره على إتيان فعل أو الامتناع عن فعل، وذلك باستخدام نظم المعلومات أو إحدى أدواتها، يعاقب بالحبس مدة لا تزيد على سنتين والغرامة التي لا تقل عن 250000 درهم ولا تزيد على 500000 درهم، أو بإحدى العقوبتين، وتزاد العقوبة للسجن المؤقت الذي لا يزيد عن 10 سنوات إذا كان التهديد يتضمن إجبار الضحية على ارتكاب جريمة أو إسناد مسائل تمس الشرف أو الاعتبار بطلب صريح أو ضمني للقيام بعمل أو الامتناع عنه، وعلى ذلك فقد اعتبرها المشرع جنحة وشددها للجناية إذا كان التهديد بارتكاب جناية أو بإسناد أمور خادشة للشرف والاعتبار .

وتنظم النيابة العامة حملات التوعية بأخطار الابتزاز الإلكتروني والوقاية من السلوكيات التي تعرض المستخدم للابتزاز عبر قنوات التواصل الاجتماعي والرد على الاستفسارات بخصوص الجريمة، كما أطلقت النيابة العامة تطبيق (مجتمعي آمن) الذي يتيح للأفراد الإبلاغ عن الجريمة التي تقع عبر مواقع التواصل الاجتماعي؛ بهدف تعزيز المشاركة المجتمعية في توفير الحماية للمجتمع من الجرائم الإلكترونية.[11]

تعتبر جريمة الابتزاز الإلكتروني ظاهرة تخترق قيم المجتمع المعاصر، كما تهدد أهداف المجتمع في ضمان سلامة أفراده، ولعل الجوهر والسبب في تجريم هذا الفعل هو الابتزاز والتهديد والضغط الذي يتم ممارسته على الضحية بتهديدها بكشف سره، وهو ما يُعَد بدوره أمرًا مشينًا، يجبر المجني عليه على الانصياع لإرادة الجاني والاستجابة لمطالبه كرهًا عنه وخوفًا من الفضيحة، مما دفع المشرع الإماراتي إلى إصدار قوانين تعاقب على هذا السلوك الإجرامي.

ويعتبر الابتزاز صورة من صور تعكير صفو الحياة وزعزعة استقرارها، وهز الشعور بالاطمئنان، الأمر الذي قد ينعكس سلبًا على حياة الفرد المبتز، مما جعل من هذه السلوكيات محلاً للتجريم من جانب المشرع الإماراتي.

(11) د . سعيد بالحاج - جريمة الابتزاز الإلكتروني - https://u.ae/fr/participate/blogs/blog?id=191

لذا فإن العقوبات الرادعة وفرض النظم والقوانين له دور فعال في مكافحة جريمة الابتزاز الإلكتروني، مما يعزز الدور الريادي لدولة الإمارات في مكافحة الجرائم الإلكترونية.[12]

المطلب الثاني: خصائص ودوافع جريمة الابتزاز الإلكتروني

الفرع الأول: خصائص جريمة الابتزاز الإلكتروني

الابتزاز كغيره من الجرائم والأفعال الآثمة الأخرى التي استفاد مرتكبوها من التقدم التقني والإلكتروني، ترتكب بالطرق التقليدية أو بالوسائل الإلكترونية. والابتزاز التقليدي هو الذي يتم من خلال وسائل تقليدية؛ مثل: مواجهة الجاني بالضحية مواجهة مباشرة، أو إرسال خطاب مكتوب بخط اليد يتضمن التهديد الذي يوجهه إليه، أو يتم إرسال التهديد من خلال شخص وسيط.

أما الابتزاز الإلكتروني فيقوم الجاني فيه باستغلال معرفته بالوسائل الإلكترونية؛ كالحاسوب الآلي، والهاتف المحمول بكافة صوره وتطبيقاته، للقيام بجريمته عبر الوسائل الإلكترونية؛ مثل إرسال رسالة تهديد عبر شبكة الإنترنت أو تطبيق الواتس آب، أو نشر الأمور التي يتم التهديد بإفشائها على وسائل التواصل الاجتماعي.[13]

ولجريمة الابتزاز الإلكتروني خصائص عديدة تتميز بها بشكل عام أو ترتبط بالوسائل الإلكترونية، وهو ما سنوضحه من خلال عرض هذه الخصائص على النحو التالي:

- تعد من الجرائم الإلكترونية؛ كونها لا تتم إلا بواسطة استخدام تقنية المعلومات، بالإستعانة بأجهزة متصلة بشبكة الإنترنت، وابتكار برامج معينة من أجل الوصول إلى البيانات الخاصة بالضحية.
- تنوع المصالح التي يلحقها الضرر من جراء ارتكاب جريمة الابتزاز، وهو ما عبر عنه البعض بِـ "تعدد المصلحة محل الحماية الجنائية"، فإذا قمنا بتحليل جريمة الابتزاز نجد من ناحية أنها عدوان على الحرية الشخصية للضحية أو المجني عليه، وقد جرم التهديد في ذاته؛ سواء اقترن بطلب أو تكليف بأمر أو لا، ومن ناحية أخرى نجد أن جريمة الابتزاز تمثل اعتداءً على ملكية المجني عليه وشرفه وسمعته، كما قد تلحق الضرر بكرامته أو بسلامته الشخصية.
- تتنوع جريمة الابتزاز الإلكتروني من حيث وقت ارتكابها إلى:

أ- جريمة وقتية؛ كأن تُهَدد امرأة شفاهةً بفضح سرها لزوجها كي يحصل منها على

(12) https: //www.munasaha.ae/ar/blogs/grym-l-btz-z-l-lktrony

(13) الطوالبة، علي (2008) الجرائم الإلكترونية، جامعة العلوم التطبيقية. مملكة البحرين، ص 60

مبلغ مالي أو منفعة غير أخلاقية، وينتهي التهديد بالتسليم، فغالبًا لا يحتاج ارتكابها إلى فترة طويلة من الزمن، مما يدفع بالجناة دائمًا إلى ارتكاب مثل هذا النوع من الجرائم بحرفية وابتكار؛ باستخدام وسائل التقنية الحديثة بهدف الحصول على المال الوفير في وقت قصير.

ب- جريمة مستمرة أو متتابعة؛ كأن يقوم المجرم بتهديد الضحية كل يوم بإفشاء أسرارها ما لم تسلم له مبلغًا من المال، أو الحصول على منفعة لا أخلاقية مستمرة.

- جريمة الابتزاز الإلكتروني من جرائم الضرر؛ إذ إنه يشترط لاكتمال السلوك الإجرامي المكون للركن المادي لهذه الجريمة أن تتحقق نتيجة معينة، بمعنى أن يقوم المجني عليه بتنفيذ المطلوب منه.
- الجناة في جريمة الابتزاز الإلكتروني غالبًا من الأصدقاء والأقارب؛ لعلمهم بمواطن الضعف لدى المجني عليه، كما أنها قد تمارس من الشريك في الجريمة المهدد بها؛ للحصول منه أو منها على مبلغ مالي، ونظرًا لتوافر هذا الاعتبار في الجناة ففي بعض الأحيان يكونون أحرص على السرية، والضحية يحاول إخفاء ما تعرض له من تهديدات من قبل الجاني خوفًا من انتشار الفضيحة بين الأصدقاء والأهل، والمقابل المطلوب القيام به من قبل المجني عليه قد يكون مشروعًا أو غير مشروع، وقد يكون عملًا أو امتناعًا عن عمل، وتتعدد مراحل الابتزاز الإلكتروني؛ حيث يمر غالبًا – أيًا كانت وسيلته- بست مراحل، هي: الطلب، والمقاومة، والضغط، والتهديد، والإذعان، والتكرار.[14]

ويرى الباحث أن الابتزاز الإلكتروني يتفرد كجريمة ضمن الجرائم الإلكترونية؛ لأنه لا يعتمد فقط على الفعل الإجرامي، بل يعتمد على استخدام التكنولوجيا بشكل متقدم ومبتكر للوصول إلى الضحية، وهذا يضع تحديات جديدة أمام الأجهزة الأمنية والمشرعين الذين يجب عليهم مواكبة تطورات هذه الجريمة التقنية.

الفرع الثاني: دوافع جريمة الابتزاز الإلكتروني

من الأسباب التي تدفع مرتكبي جرائم الابتزاز الإلكتروني لارتكاب جرائمهم تحقيق الربح المادي، أو الرغبة في إثبات الذات، كذلك الدافع في إقامة علاقة غير أخلاقية، وذلك بسبب عدم قدرته على بناء علاقات اجتماعية سوية، كما يمكن أن تكون دوافع الجناة

(14) جاسم ناصر جاسم المسلماني - التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري – مرجع سابق – ص11ص19

خارجية، كأن تدفع الحاجة بعض المنظمات أو الدول للاتصال بشاغلي الأماكن الحساسة في منظماتهم للعمل لدى منظمات أو دول أخرى للحصول على المعلومات والتقنيات المتوفرة لديهم، ويقوم لتحقيق ذلك برشوة أو إقناع أو إغراء الشخص المستهدف، وإذا رفض المغريات تعرض للابتزاز الإلكتروني بالوسائل المختلفة. وبناءً على ما سبق ستتم مناقشة الدوافع المادية وغير الأخلاقية والانتقامية والخارجية، على النحو التالي:

أولاً: دافع الحصول على المال[15]:

إذا كانت دوافع الجاني في جريمة الابتزاز الإلكتروني مالية فإن الجاني يهدد المجني عليه لتسليم نقود له، أو أشياء ذات طابع مادي باستخدام نظم المعلومات المختلفة، فيقوم الجاني بذلك بطريقة مباشرة؛ كأن يطلب الجاني المال مباشرة من المجني عليه، فيطلب منه تحويل مبالغ مالية بشكل مستمر له أو لغيره، أو بطريقة غير مباشرة كأن يطلب من المجني عليه تسديد مبلغ مالي كان قد اقترضه من البنك، أو دفع أقساط سيارة، أو يطلب منه القيام بكشف أسرار الشركة التي يعمل لديها، أو معرفة الأرقام السرية لحسابات الشركة، أو بإطلاق الشائعات ونشرها عنه إذا امتنع عن دفع المبالغ المالية التي يطلبها الجاني، أو عدم تلبية طلباته بهدف تركهم والابتعاد عنهم، مع الوعد بعدم التعرض لهم وعدم تشويه سمعتهم.

ثانيًا: الدوافع غير الأخلاقية[16]:

وقد يكون الدافع غير أخلاقي، وهو ما تتسم به هذه الجريمة في غالب أنماطها؛ حيث يقوم الجاني بتهديد المجني عليه بفضح أمره، أو إفشاء سره، أو الإبلاغ عنه مستغلاً ضعفه أمام تهديداته، وينقسم الابتزاز الجنسي إلى ابتزاز جنسي إلكتروني، ويتحقق عن طريق وسائل الاتصال عبر الإنترنت مثل ماسنجر فيس بوك، أو سكاي بي، أو مواقع الزواج، أو مواقع التوظيف، ويعد الجاني في هذه النوعية من الابتزاز مجرمًا خفيًا يسعى للوصول إلى معلومات حساسة للضحية، أما الابتزاز الواقعي فيتم عندما يقوم الجاني بجمع معلومات عن الضحية مستغلاً علاقته بها كالتقاط صور تسيء للضحية وهي بصحبته، أو أن يحصل على هذه المعلومات أو الوثائق السرية أو المقاطع الصوتية أو المرئية التي تخص المجني عليها بأساليب احتيالية، أو يحصل من الضحية على الأرقام السرية لبطاقات ائتمان ولي أمره دون علمه، ويهدده بفضح أمره في حال عدم تلبية طلباته غير الأخلاقية بتهديده بنشر تلك الوثائق.

(15) Paganini, P. (2018). "Understanding the motives behind cyber extortion: A deep dive into ransomware attacks." Journal of Information Security and Applications, 43, 2332-, DOI: 10.1016/j.jisa.2018.06.004

(16) Holt, T.J., & Smirnova, O. (2014). "Exploring the market for cybercrime tools: Characteristics of buyers and sellers in a digital underground economy." Journal of Criminal Justice, 42(1), 2738-, DOI: 10.1016/j.jcrimjus.2013.11.005

ثالثًا: دافع الانتقام:

يتحقق الدافع الانتقامي بتلذذ الجاني بأذية المجني عليه واستمتاعه بتوسلاته وحتى ببكائه، ومما يزيد الأمر سوءًا أن يقوم الجاني بتصوير المجني عليه ويطلب منه ذكر اسمه أو أي بيانات تتعلق به، كما قد يكون الدافع لدى الجاني هو الانتقام من المجني عليه عن طريق إلحاق الأذى به وإساءة سمعته بنشر صوره؛ إما عن طريق شبكة الإنترنت، أو عن طريق الهواتف الذكية المزودة بكاميرا، أو عن طريق خدمة الواتس آب، والتي تعتبر من أحدث الطرق في الزمن الحاضر لسرعة انتشارها، أو أن يقوم الجاني بابتزاز المجني عليه إذا كان أنثى؛ بمنعها من الزواج بهدف الإضرار بها أو الانتقام منها.

رابعًا: دافع تحقيق الاستفادة:

يتمثل في تصوير بعض الأشخاص في المناصب الحساسة (العسكرية مثلاً) في أوضاع غير أخلاقية، وبعد ذلك يتم اللجوء إلى تهديدهم وإجبارهم على إفشاء معلومات سرية تتعلق بأمن الدولة، أو التصنيع العسكري، والأسرار والتحركات للقطع العسكرية[17].

وقد تلجأ بعض الشركات الكبرى من أجل المنافسة إلى استغلال عاملين لدى شركات منافسة أخرى للحصول على بيانات مالية أو معلومات إدارية حول وضع الشركة المالي أو تعثرها الإداري ومشاكل تعيق استمرار نشاطها في السوق، وتهديدهم وابتزازهم من أجل الحصول على هذه المعلومات عن الشركات المنافسة، لاستغلالها في تحقيق مكاسب سوقية وتعطيل نمو الشركات المنافسة، أو الحصول على معلومات عن أسرارها الصناعية أو التجارية أو مصادر البضاعة فيها أو الأسعار الحقيقية للسلع.

ويرى الباحث أن الدوافع التي قد تدفع المبتز إلى ارتكاب جرائمه تتضمن دوافع مادية، وهي رغبته في الحصول على المال باستغلال أسرار وخصوصيات الآخرين التي ينشرونها عن غير وعي بمخاطر نشرها أو تبادلها مع الآخرين، أو استدراج الضحية إلى إفشاء أسرارها ثم استغلالها بعد ذلك، أو نفسية تتمثل في الرغبة في إذلال الآخرين سواء لدوافع انتقامية أو لأسباب نفسية لدى الجاني، أو اجتماعية بسبب التفكك الأسري، أو الرغبة في إكراه الآخرين على علاقات اجتماعية غير مرغوبة نظرًا لعدم قدرة المبتز على الانخراط في علاقات اجتماعية صحية وسليمة.

(17) أطروحة ماجستير بعنوان "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي " الفيسبوك نموذجًا" دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال – جامعه قاصدي مرباح " تخصص تكنولوجيا الاتصال الجديدة – الجزائر – مقدمة من سمان جويدة، إيمان مردف 2017م – ص23ص25 - https: //dspace.univ-ouargla.dz/jspui/ samane-mardaf.pdf/1/14448/bitstream/123456789

الفرع الثالث: أنماط ومحاور الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

أولاً: أنماط الابتزاز عبر مواقع التواصل الاجتماعي:

تستخدم مصطلحات الابتزاز والابتزاز الجنسي بانتظام بشكل تبادلي، على الرغم من اختلاف معانيها؛ حيث إن الابتزاز ينطوي على استخدام القوة والعنف أو التهديد باستخدامها للحصول على أموال نقدية أو سلع أخرى ذات قيمة، كما يتضمن الابتزاز الإكراه من خلال التهديد بكشف معلومات حول الضحية للآخرين، وإن الابتزاز الإلكتروني ينطوي على تهديد الضحايا بتدمير الممتلكات أو البيانات[18]، كما ينطوي على الإكراه من خلال التهديد بإفشاء معلومات حساسة عن الضحية يمكن أن تضر بسمعتهم، وتم تعريف المعلومات الحساسة بأنها: "المعلومات التي يمكن استخدامها لتمكين الخصوصية أو الإضرار بالأمان عند وضعها في الأيدي الخطأ"، فيمكن أن يشمل الابتزاز الإلكتروني اختراق جهاز كمبيوتر والتهديد بإتلاف البيانات، كما يتضمن ممارسة السلطة على الضحايا بتهديدهم بنشر معلومات حساسة يمكن أن تضر بسمعتهم إذا لم يمتثلوا لمطالب الجاني.

أما مصطلح Sextortion فيشمل أحد أنماط الابتزاز الإلكتروني الذي يقوم على استخدام البيانات غير الأخلاقية للضحايا [19] على مواقع التواصل الاجتماعي، فيتمكن الجناة من الحصول على معلومات حساسة من خلال تحليل محتوى حسابات وسائل التواصل الاجتماعي، أو إهمال المستخدم، أو الاستيلاء على هذه البيانات من الضحايا عن عمد ووعي. ومن الملاحظ أن الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي صار أكثر شيوعًا؛ حيث يتم جمع المعلومات عادةً من الملفات الشخصية على وسائل التواصل الاجتماعي أو الاستيلاء عليها بخداع المستخدمين؛ فَقَد أفادت بعض الإحصاءات أن 6 إلى 8 بالمائة من الشباب التشيكي (الذين تتراوح أعمارهم بين 8 و17 عامًا) تعرضوا للابتزاز على مواقع التواصل الاجتماعي؛ حيث طلب المبتزون الأموال وعلاقات غير أخلاقية أو صور فاضحة للضحية وأشياء أخرى من الضحايا، وفي حالات ابتزاز أخرى عبر مواقع التواصل الاجتماعي انتحر الضحايا بسبب الابتزاز، كما أفادت دراسة بزيادة حالات الابتزاز على مواقع التواصل الاجتماعي في دول مجلس التعاون الخليجي؛ إذ يتم الإبلاغ عن 30 ألف حادثة من هذا القبيل سنويًا من قبل دول مجلس التعاون الخليجي، و80 بالمائة من هذه الحوادث تتعلق باستهداف النساء بمحتوى غير أخلاقي. كما أن ابتزاز الأطفال على وسائل

(18) Wang, Y., & Stefanone, M. A., "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality", New Media & Society, 2022., pp: 535541-

(19) Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525540-. https: //doi.org/10.1057/s412842-00246-020-

التواصل الاجتماعي يتم فيه استخدام الأدلة أو الصور المثيرة للحصول على فوائد حسية أو أموال نقدية، وقد ارتفع هذا الأمر أيضًا بشكل كبير في العقد الماضي.

ومن أنماط الابتزاز الإلكتروني ما تتعرض له المؤسسات عبر مواقع التواصل الاجتماعي؛ حيث يهدد الأفراد بتشويه سمعتها فيطلب المبتزون الأموال أو الخدمات غير الأخلاقية أو أداء خدمة مشروعة أو غير مشروعة، ولا شَكَّ أن الوقوع ضحية للابتزاز يمكن أن يشوه اسم الضحية وسمعة عائلته، كما قد يؤدي إلى ضائقة نفسية قد تصل إلى الانتحار، ويمكن أن يساهم هذا الأمر في ازدياد مشاعر القلق أو الخوف أو الاكتئاب أو اضطرابات التكيف الاجتماعي التي قد تؤدي إلى العزلة الاجتماعية والخوف من مواجهة الناس.

وبالنسبة للأطفال، يمكن أن تشمل الآثار الجانبية لوم الذات، والذكريات أو المشاعر الغازية، والتعاسة، وتدني احترام الذات، والأحلام السيئة، والأرق، والعصبية، ونوبات القلق، والصعوبات التعليمية. وعلى الرغم من هذه العواقب، تشير الأبحاث إلى أن الناس غالبًا ما يكونون عرضة لأن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي؛ بسبب ميلهم إلى الكشف عن معلومات حساسة عبر الإنترنت.[20]

الإفصاح عن الشخصية الحقيقية عبر مواقع التواصل الاجتماعي يتضمن مشاركة معلومات حساسة مع أشخاص آخرين فهو نشاط متعمد يشارك فيه الشخص ممارساته الشخصية وصوره وعواطفه مع الآخرين، وتم تعريف الكشف عن الذات عبر الإنترنت على أنه الكشف عن الذات الذي يحدث عبر الإنترنت، ويتم الترويج للإفصاح الذاتي عبر الإنترنت من خلال منصات وسائل التواصل الاجتماعي نظرًا لقيمته التجارية.

ويركز المجرمون وأعضاء جماعات الجريمة المنظمة على استخدام مواقع التواصل الاجتماعي لابتزاز المستخدمين بسبب الميل الأكبر لمستخدمي مواقع التواصل الاجتماعي للكشف عن شخصياتهم الحقيقية على مواقع التواصل الاجتماعي، وقد سعت جهود مكافحة الابتزاز على مواقع التواصل الاجتماعي للحد من هذه الجرائم من خلال رفع مستوى الوعي بمخاطر استخدام الإنترنت، وتقديم المشورة حول كيفية تجنب الوقوع ضحية لهذا الجرائم، وتسعى هذه الحملات للحد من مشاركة المعلومات الشخصية الحساسة على مواقع التواصل الاجتماعي، ومع ذلك يستمر المستخدمون في تبادل هذه المعلومات.

(20) Authors. Alma Spaniardi, Janki Modi Avari, Teens, Screens, and Social Connection An Evidence-Based Guide to Key Problems and Solutions, 2023, Jenna Margolis and Dinara Amanbekova, Social Media and Cyberbullying, pp: 81: 83, https: //doi.org/10.10077-24804-031-3-978/

إنَّ بعض الأسباب المطروحة لتفسير الإفصاح عن الشخصية والبيانات عبر مواقع التواصل الاجتماعي تتضمن الفشل في فهم مخاطر مشاركة المعلومات الحساسة، والتركيز على متعة الانخراط في هذا النشاط وإمكانية السماح للعلاقات بالتطور[21].

ويرى الباحث أن أنماط الابتزاز الإلكتروني أصبحت أكثر تعقيدًا وانتشارًا مع تزايد استخدام وسائل التواصل الاجتماعي، وأن الجرائم التي تستهدف الضحايا عبر الإنترنت ليست مادية أو غير أخلاقية فقط، بل لها تداعيات نفسية واجتماعية خطيرة قد تصل إلى الانتحار، وإنَّ الجهود المبذولة للحد من هذه الجرائم تحتاج إلى تعزيز الوعي حول مخاطر الكشف عن الذات عبر الإنترنت، وتعليم الأفراد كيفية حماية خصوصياتهم على هذه المنصات.

ثانيًا: محاور الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي:

1- التعرض للإيذاء:

تم تحديد العمر والجنس والميل إلى الكشف عن الذات عبر الإنترنت والرغبة في استخدام وسائل التواصل الاجتماعي لإرسال صور حميمة كعوامل خطر للوقوع ضحية للابتزاز على وسائل التواصل الاجتماعي. وكان الشباب أكثر عرضة لخطر الوقوع ضحية لهذا النشاط من كبار السن، ويعتقد أن الأشخاص الذين تتراوح أعمارهم بين 15 و25 عامًا هم الأكثر عرضة للخطر[22]، ويعتقد أيضًا أن الإناث أكثر عرضة للخطر من الذكور بسبب ميل الإناث إلى التعرض لضغوط أكبر لنشر صور حميمة لأنفسهن على وسائل التواصل الاجتماعي.

كما لوحظ وجود علاقة بين الانخراط في الإفصاح عن البيانات الشخصية والوقوع ضحية للابتزاز على مواقع التواصل الاجتماعي؛ حيث إن الذين يكشفون عن معلوماتهم الشخصية أكثر عرضة للوقوع ضحية للابتزاز، كما أن مشاركي الصور الشخصية الجنسية معرضون لخطر الوقوع ضحية للابتزاز على مواقع التواصل الاجتماعي[23]، كما أن عدم الوعي بمخاطر استخدام مواقع التواصل الاجتماعي فيما يتعلق بالتبعات القانونية لإنشاء ومشاركة صور غير أخلاقية للأطفال، فضلاً عن تصميم وسهولة استخدام تطبيقات الوسائط الاجتماعية، يزيد من احتمالية إنشاء مثل هذه الصور ومشاركتها، وبالتالي الوقوع

(21) Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats" by Will Gragido, John Pirc, Nicholas Hoffman, & Daniel Molina, Syngress, 2011, pp: 2022-

(22) Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Routledge, 2017,

(23) Abdullah Al Habsi · Michelle Butler · Andrew Percy, Blackmail and the self-disclosure of sensitive information on social media: Prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users", Security Journal, 2023, pp: 250: 252, https: //doi.org/10.1057/s412843-00376-023-

ضحية للابتزاز. ويمكن أن يؤدي تصميم تطبيقات الوسائط الاجتماعية وسهولة استخدامها أيضًا لزيادة التعرض للابتزاز من خلال الترويج لمزيد من الإفصاح عن الهوية الحقيقية للمستخدمين، وسهولة إنشاء الصور غير الأخلاقية وتوزيعها، ودوام الصور ومستوى الأمان بإنشاء حسابات الوسائط الاجتماعية، فالتطبيقات التي شجعت ميزاتها على الكشف عن المعلومات والصور، وجعلت إنشاء الصور وتوزيعها أسهل، واحتفظت بالصور وسمحت بإنشاء حسابات بمعلومات كاذبة، يمكن أن تسهل حدوث الابتزاز.

2- التباين الثقافي في الوعي:

إنَّ الدليل على الدور المهم الذي يمكن أن تؤديه المعايير الثقافية في تشكيل مواقف الناس ودوافعهم للانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي واضح أيضًا، فضلاً عن وعيهم باحتمال أن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي. وقد أشارت الدراسات التي أجريت في الدول الغربية إلى أن الناس غالبًا ما يشعرون بأن المعايير الثقافية تشجع على نشر المحتوى غير الأخلاقي على حسابات وسائل التواصل الاجتماعي؛ حيث يسعى الناس إلى زيادة جاذبيتهم وتفاعلاتهم مع المستخدمين الآخرين على وجه الخصوص، وأبلغت الإناث أنه طلب منهن مشاركة صور حميميَّة؛ حيث ذكر البعض أنهن شعرن بالضغط لمشاركة مثل هذه الصور من أجل الحفاظ على تفاعلاتهن، ومع ذلك أفاد مستخدمو وسائل التواصل الاجتماعي في الدول الغربية بأنهم أقل وعيًا باحتمال حدوث ابتزاز أو الإضرار بالسمعة نتيجة لمشاركة مثل هذه المعلومات على وسائل التواصل الاجتماعي، في المقابل تميل المعايير الثقافية في البلدان العربية إلى الحد من نشر المحتوى غير الأخلاقي على مواقع التواصل الاجتماعي وخاصة بالنسبة للنساء؛ حيث تميل النساء إلى مواجهة ضرر أكبر بسمعتهن ومكانة اجتماعية منخفضة إذا انخرطن في مثل هذا السلوك، ونتيجة لذلك فإنهن أكثر وعيًا باحتمال حدوث ابتزاز وإلحاق الضرر بالسمعة إذا شاركوا معلومات شخصية حساسة على وسائل التواصل الاجتماعي، وقد أدت هذه المعايير الثقافية والعواقب الاجتماعية المحتملة التي قد تتبع مثل هذا الإفصاح إلى التعبير عن مخاوف جدية بين النساء العربيات بشأن خصوصيتهن على وسائل التواصل الاجتماعي، وكيف يمكن استخدام المعلومات التي شاركنها لابتزازهن من قبل مستخدمي وسائل التواصل الاجتماعي الآخرين، وعلى الرغم من هذه المخاوف، تم اقتراح المعايير الثقافية التي تقيد تطور العلاقات خارج الإنترنت في الثقافات العربية، وخاصة بالنسبة للنساء، لتحفيز الناس على الانخراط في الكشف عن الذات بشكل أكثر حرية وانفتاحًا على

وسائل التواصل الاجتماعي؛ حيث استخدموا وسائل التواصل الاجتماعي لتطوير علاقات جديدة، متحررين من القيود التي يواجهونها في تعاملاتهم الاجتماعية في المجتمع.[24]

وعلى الرغم من الوعي المتزايد باحتمال حدوث الابتزاز وعواقبه الخطيرة، فقد استمر الناس في الثقافات العربية في تعريض أنفسهم لخطر الابتزاز على وسائل التواصل الاجتماعي أثناء سعيهم لبدء علاقات جديدة مرغوبة، وتثير مثل هذه الأبحاث تساؤلات حول مدى نجاح حملات التوعية في تغيير السلوك وتقليل مخاطر الابتزاز على وسائل التواصل الاجتماعي، فضلاً عن إظهار الحاجة إلى مزيد من البحث لفهم كيفية تفاعل الأعراف والمواقف والمعتقدات الثقافية مع بعضها البعض للتأثير على السلوك.

3- استخدام الإكراه في الابتزاز:

تم استخدام أسلوبين رئيسين من المبتزين للحصول على معلومات حساسة من ضحاياهم، الأول حيث قام الضحايا بمشاركة معلومات أو صور حساسة مع المبتز أو قام المبتز بتسجيلها أثناء مشاركتهم طوعًا في نشاط حساس عبر كاميرا الويب فقط، وعندما انهارت هذه العلاقات أو عندما لم يعد الضحايا على استعداد لمشاركة المعلومات أو الصور أو مقاطع الفيديو الحساسة مع مرتكب الجريمة، بدأ الابتزاز مع إجبار الضحايا على إعادة بدء العلاقة أو الاستمرار في الكشف عن معلومات حساسة.

الثاني هو الصور أو مقاطع الفيديو؛ حيث يقوم المبتز بالتلاعب عاطفيًا بالضحية للكشف عن معلوماتها الحساسة بالادعاء بأنه مكتئب أو لديه ميول انتحارية ومحاولة إثارة الشعور بالذنب أو الالتزام لدى الضحية لمساعدتها من خلال مشاركة هذه البيانات، وقد تبين أن البالغين والشباب - على حد سواء- كانوا ضحايا لهذه الأساليب الإكراهية.

وتبين أيضًا من الحالات العديدة أن الشباب الذين يقعون ضحايا للابتزاز على مواقع التواصل الاجتماعي هم أكثر عرضة للإبلاغ عن استخدام هذه الأساليب الإكراهية ضد الآخرين، مما يؤدي إلى إدامة الانتهاكات، ومع ذلك فمن غير الواضح ما إذا كان البالغون يواجهون دورة مماثلة من الضحية إلى الجاني، أو ما هي الآليات التي قد تسبب هذا التحول.[25]

(24) Tommy K.H. Chan, Christy M.K. Cheung, Zach W.Y. Lee, Cyberbullying on Social Networking Sites : A Literature Review and Future Research Directions" , Information & Management, Volume 58, Issue 2, March 2021, 103411, pp: 12: 14 https: //www.sciencedirect.com/science/article/pii/S0378720620303499?via%3Dihub

(25) Nash, M. (2020). "Coercion, Consent, and the Criminal Law: Understanding the Limits of Criminal Liability." Criminal Law Review, 1, 2439-. DOI: 10.2139/ssrn.3563456

4- الكشف عن الذات على وسائل التواصل الاجتماعي:

تم التحقيق في الكشف عن الذات على وسائل التواصل الاجتماعي من بين 67 دراسة تمت مراجعتها، فحصت الأغلبية (41 من أصل 67) بشكل مباشر سبب مشاركة الأشخاص في الكشف عن أنفسهم على وسائل التواصل الاجتماعي أو العوامل التي يمكن أن تزيد من احتمالية انخراط الفرد في هذا السلوك، وركز الباقي على استخدام وسائل التواصل الاجتماعي بشكل عام، مع الإشارة إلى الكشف عن الذات ضمن النتائج التي توصلوا إليها.

وقد بينت الدراسات أن الإفصاح عن الذات مرتبط بالوقوع ضحية للابتزاز عبر مواقع التواصل الاجتماعي؛ حيث أشارت إلى أن الإفصاح عن الهوية الحقيقية عند التواصل عبر مواقع التواصل الاجتماعي يزيد من مخاطر الوقوع ضحية للابتزاز، وسلطت الضوء على قدرة المعايير الثقافية على تشكيل المواقف ودوافع الانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي.

وحددت الدراسات في هذا المجال ثلاثة مواضيع رئيسة: الحاجة إلى العلاقات والكشف عن الشخصية، والانفصال بين المخاوف المتعلقة بالخصوصية والكشف عن الشخصية عبر الإنترنت، وتأثير ميزات المنصة على الكشف عن الشخصية. وإنَّ الحاجة إلى العلاقات والتعبير عن الشخصية هو أحد أكبر العوامل التي تؤثر على الكشف عن الشخصية على وسائل التواصل الاجتماعي، وهو الدافع لدى الشخص لاستخدام وسائل التواصل الاجتماعي. كما قرر العديد من مستخدمي مواقع التواصل ممن يفصحون عن شخصياتهم الحقيقية عبر الإنترنت برغبتهم في استخدام وسائل التواصل الاجتماعي للحفاظ على العلاقات، وهو ما دعاهم للتواصل مستخدمين هوياتهم الحقيقية لتعميق صداقاتهم واكتساب المكانة الاجتماعية أو القبول أو الدعم والتحقق من الصحة[26].

كما تبين بعض الدراسات أن مستخدمي مواقع التواصل يقومون بالإفصاح عن معلوماتهم الشخصية لإدارة الانطباع الذي تولد لدى الآخرين؛ حيث يكشف المستخدمون عن المعلومات التي تساعدهم في تحقيق أهداف علاقتهم، بينما يرغب مستخدمو مواقع التواصل الاجتماعي في التعبير عن الذات للإفصاح التلقائي أثناء تعبيرهم عن أنفسهم عبر الإنترنت.[27] على وجه الخصوص، الأشخاص الذين عاشوا في البيئات التي أيدت

(26) "Coercion and Responsibility in Criminal Law: A Study of the Limits of Criminal Liability" by Douglas Husak, Oxford University Press, 2020, pp: 22: 24

(27) Pemberton, A., Winkel, F.W., & Groenhuijsen, M.S. (2007). "Taking victims seriously in restorative justice: A crime victim and human rights perspective." European Journal of Crime, Criminal Law and Criminal Justice, 218220-.

العادات الاجتماعية التي تفرض ضوابط سلوكية وأخلاقية في المجتمع خارج الإنترنت، كانوا يستخدمون مواقع التواصل الاجتماعي للتعبير عن ذواتهم "الحقيقية" والانخراط في الكشف عن الذات عبر الإنترنت كوسيلة لتلبية احتياجاتهم التعبيرية والعاطفية، كما هو الحال مع الدراسات التي تبحث في الابتزاز عبر مواقع التواصل الاجتماعي، فقد سعت العديد من الدراسات أيضًا إلى تحديد مخاطر كشف مستخدمي مواقع التواصل الاجتماعي لشخصياتهم الحقيقية؛ حيث توصلت هذه الدراسات إلى أن العمر والانفتاح وضبط النفس والكفاءة الذاتية أثرت على كمية ونوعية البيانات الشخصية والمعلومات التي يقوم مستخدمو مواقع التواصل الاجتماعي بالإفصاح عنها.

أما الذين كانوا أصغر سنًّا وأكثر انفتاحًا، فقد كانت لديهم مستويات أقل، بينما كان ضبط النفس وزيادة الكفاءة الذاتية في استخدام وسائل التواصل الاجتماعي والتلاعب بها أكثر عرضة لكشف معلوماتهم على وسائل التواصل الاجتماعي، وبالتالي فإن الدوافع الكامنة وراء استخدام مواقع التواصل الاجتماعي، بالإضافة إلى الخصائص الفردية مثل العمر والشخصية والسمات النفسية، يمكن أن تؤثر على مقدار ونوع الكشف عن الذات الذي يشارك فيه الأشخاص على وسائل التواصل الاجتماعي، وكشفت الدراسات أيضًا أن الناس كانوا قلقين بشأن خصوصيتهم على وسائل التواصل الاجتماعي.[28]

أما معظم الدراسات التي تبحث في كيفية تأثير المخاوف المتعلقة بالخصوصية على الميل إلى الانخراط في الكشف عن الذات على وسائل التواصل الاجتماعي، فلم تتوصل إلى أي دلائل على أن المخاوف المتعلقة بالخصوصية تؤثر بشكل مباشر على سلوك الكشف عن الذات، وعند تحديد موعد الكشف عن المعلومات على وسائل التواصل الاجتماعي كان الناس يميلون إلى الانخراط في تحليل التكلفة والعائد للإيجابيات والسلبيات التي يعتقدون أنها مرتبطة بالمشاركة في الكشف عن الذات عبر الإنترنت.[29]

ثم توصل هذا التحليل إلى تقليل الجوانب السلبية عند اتخاذ القرار بشأن ما إذا كان سيتم الكشف عن المعلومات على وسائل التواصل الاجتماعي أم لا؛ حيث تم التقليل من أهمية السلبيات المترتبة على الإفصاح عن الشخصية عبر الإنترنت، في حين تمت المبالغة

(28) د. هشام رشدي خير الله – ادراك المراهقات لمخاطر الابتزاز الإلكتروني عبر الانترنت وتأثيره على اتجاهاتهم نحو استخدام تطبيقات التواصل الاجتماعي عبر الهواتف الذكية "دراسة في ضوء مجتمع المخاطر" – المجلة العلمية لبحوث الصحافة – عدد 24 – الجزء الاول – يوليو 2022 – ص123

(29) "The Impact of Self-Disclosure on Social Media on Personal Relationships: A Cross-Cultural Analysis" by Bazarova, N. N., & Choi, Y. H., Journal of Communication, 2020., DOI: 10.1093/joc/jqz052

فـي تقديـر الـمنفعة الـمترتبة على الإفصـاح عـن الشـخصية الحقيقيـة فـي العلاقـات والتعبيـر عـن الـذات، ومـع ذلـك يمكـن أن تؤثـر الـمخاوف الـمتعلقة بالخصوصيـة على موقـع التواصـل الاجتماعـي الـذي يسـتخدمه الشـخص ومـدى تفعيـل ضوابـط الخصوصيـة فـيها، فـيمكن أن تشـجع الـمخاوف الـمتعلقة بالخصوصية الـمستخدمين على الحد من ظهور ملفاتهم الشـخصية على وسـائل التواصـل الاجتماعـي، وتقييـد تفاعلاتهـم مـع مسـتخدمين غيـر معروفـين.

وعلـى الرغـم مـن الـمخاوف الـمتعلقة بالخصوصيـة، لا يـزال الـمستخدمون يكشـفون عـن معلوماتهـم الشـخصية علـى مواقـع التواصـل، ممـا يمكنهـم مـن عـرض ملفاتهـم الشـخصية للـمتفاعلين معهـم، ممـا يعـزز مـن تأثيـر الـمخاوف الـمتعلقة بالخصوصيـة علـى مـا كان مرئيًـا للعامـة ومـع تفاعـل الـمستخدمين، وليـس نوعيـة أو كـم الـمعلومات التـي كشـفوا عنهـا.

كمـا أنـه بـدلاً مـن أن تؤثـر مخـاوف انتهـاك الخصوصيـة علـى كـم الـمعلومات الشـخصية التـي يتـم مشـاركتها عبـر مواقـع التواصـل الاجتماعـي، فـإن مـدى الكشـف عـن البيانـات الشـخصية عبـر الإنترنـت مقبـول اجتماعيًـا، فـإذا كان الإفصـاح عـن الشـخصية الحقيقيـة للـمستخدم مقبـول اجتماعيًـا بيـن الـمستخدمين، فإنهـم يكونـون أكثـر ميـلاً لذلـك.

وقـد أكـدت الدراسـات العديـد مـن الـمخاوف بشـأن فعاليـة رفـع الوعـي للحـد مـن التعـرض للابتـزاز، فركـزت علـى تزايـد مخـاوف انتهـاك خصوصيـة الـمشاركين كوسـيلة لتقليـل احتمـال تعرضهـم للوقـوع ضحايـا لجرائـم الابتـزاز الإلكترونـي، وقـد حققـت هـذه التـدخلات نجاحًـا محـدودًا بسـبب اخـتلاف مخـاوف الخصوصيـة وبيـن الـمشاركة فـي الإفصـاح عـن الشـخصية عبـر الإنترنـت فـي هـذه الدراسـات.[30] بـل يمكـن أن تحقـق التـدخلات نجاحًـا أكبـر مـن خـلال العمـل علـى تغييـر التقاليـد الاجتماعيـة التـي تقبـل وتشـجع الكشـف عـن الـذات علـى مواقـع التواصـل الاجتماعـي.

وفـي تأثيـر ميـزات النظـام الأساسـي على الكشـف عن الذات، كان الـموضوع الرئيسـي الأخيـر الـذي بـرز مـن هـذه الدراسـات هـو التأثيـر الـذي يمكـن أن تحدثـه ميـزات النظـام الأساسـي لتطبيقـات الوسـائط الاجتماعيـة علـى الـميل إلـى الـمشاركة فـي الكشـف عـن الذات على وسـائل التواصـل الاجتماعـي.[31]

(30) Self-Disclosure and Psychological Well-Being in the Age of social media: A Meta-Analysis" by Nguyen, M. H., Bin, Y. S., & Campbell, A., Cyberpsychology, Behaviour, and Social Networking, 2021., DOI: 10.1089/cyber.2020.0329

(31) "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality" by Wang, Y., & Stefanone, M. A., New Media & Society, 2022., DOI: 10.1177146144482110451 48/

وقد تبين أن مقدار وطبيعة ضوابط الخصوصية المتاحة في تطبيقات الوسائط الاجتماعية المختلفة تعمل على توليد الثقة، فكلما شعر المستخدمون بثقة أكبر في هذه التطبيقات، زاد ميلهم إلى الإفصاح عن أنفسهم عبر الإنترنت، بالإضافة إلى ذلك فإن مدى شعور الأفراد بأنهم يستطيعون الثقة في المستخدمين الآخرين لتطبيقات وسائل التواصل الاجتماعي أثر على سلوكهم في الكشف عن الذات، مع ارتباط مشاعر الثقة الأكبر بمزيد من الإفصاح عن الذات.

إن مدى إمكانية تشفير المحتوى، وسهولة التقاط الصور ومشاركتها مع الآخرين، وما إذا كان المحتوى مؤقتًا أو دائمًا بطبيعته، أثر أيضًا على مدى الكشف عن الذات على وسائل التواصل الاجتماعي، فإذا كان المحتوى مشفرًا، فهذا يسمح للمستخدمين بالشعور بالتحكم في الأشخاص الذين يشاركون معلوماتهم معهم، ويمكن أن يؤدي إلى مزيد من الاتصال عبر الإنترنت الكشف عن الذات، وكان هذا على الرغم من إمكانية قيام مستخدمين آخرين بمشاركة هذا المحتوى دون موافقتهم. وبالمثل إذا كانت تطبيقات الوسائط الاجتماعية سهلة الاستخدام ومجانية وتسهل مشاركة الصور، فإن ميزات التصميم هذه تميل إلى تشجيع المزيد من الكشف عن الذات ومشاركة الصور.

بالإضافة إلى ذلك، إذا اعتقد الأفراد بأن صورهم وبياناتهم ستتم مشاركتها مع الآخرين مؤقتًا مثل Snapchat، فإنهم يميلون إلى أن يكونوا أكثر حرمانًا من الإفصاح عن أنفسهم عبر الإنترنت، ويمكن أن تؤثر أيضًا ميزات التصميم والمنصة المختلفة لتطبيقات الوسائط الاجتماعية على الغرض الذي يستخدمه الأفراد لتطبيقات الوسائط الاجتماعية، وبالتالي مقدار ونوع الكشف الذاتي عبر الإنترنت الذي يشارك فيه المستخدمون في هذا التطبيق.[32]

أخيرًا، إذا كان الأفراد راضين عن التصميم وميزات النظام الأساسي لتطبيقات الوسائط الاجتماعية، فمن المرجح أيضًا أن يقوموا بالإفصاح عن أنفسهم بهذه الطريقة، ومن الضروري النظر في كيفية تأثير ميزات التصميم والمنصة لتطبيقات الوسائط الاجتماعية بشكل مختلف على الإفصاح عن الذات، ونتيجة لذلك قد تختلف قابلية تعرض مستخدمي الوسائط الاجتماعية لأن يصبحوا ضحية للابتزاز على وسائل التواصل الاجتماعي، اعتمادًا على تطبيق الوسائط الاجتماعية الذي يستخدمونه.[33]

(32) Utz, S., Muscanell, N., & Khalid, R., "Self-Disclosure on Social Media: The Role of Intrinsic versus Extrinsic Motivations", Computers in Human Behaviour, 2021, pp: 1214-

(33) Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525540-. https: //doi.org/10.1057/s412842-00246-020-

ويرى الباحث أن محاور الابتزاز الإلكتروني عبر وسائل التواصل الاجتماعي تسلط الضوء على عوامل متعددة تسهم في وقوع الأفراد ضحية لهذه الجريمة، وهناك تأثير واضح للثقافة، والعمر، والجنس، والدوافع الشخصية على احتمالية التعرض للابتزاز. ومع ذلك يظهر أن مشكلة الابتزاز الإلكتروني لا تتعلق فقط بالوعي بالمخاطر، بل أيضًا بالرغبة في استخدام وسائل التواصل الاجتماعي لتحقيق أهداف شخصية وعاطفية. وبناءً على ذلك قد تحتاج حملات التوعية إلى معالجة هذا التناقض بين المخاوف المتعلقة بالخصوصية والرغبة في التعبير عن الذات عبر الإنترنت.

المبحث الثاني
إجراءات التحقيق في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

التمهيد:

تمثل جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي تحديًا متزايدًا في العصر الرقمي؛ حيث تتنوع أشكال وأساليب هذه الجرائم لتشمل التهديد بنشر معلومات شخصية أو صور خاصة مقابل الحصول على المال أو غيره من المكاسب. وتستغل هذه الجرائم التواصل المفتوح عبر الإنترنت للوصول إلى ضحايا من جميع الفئات العمرية، مما يزيد من صعوبة ضبط مرتكبيها وتقديمهم للعدالة. وتتطلب إجراءات التحقيق في هذا النوع من الجرائم تجهيزات خاصة وفهمًا عميقًا لتقنيات التحقيق الرقمي وأدواته، بهدف جمع الأدلة الإلكترونية وتوثيقها، وتتبع المجرمين، وتقديمهم للمحاكمة. من هنا، تبرز أهمية تطوير المهارات التقنية والقدرات التحليلية لدى جهات إنفاذ القانون، وتبني استراتيجيات متقدمة للتصدي لهذه الظاهرة المتنامية، وتعزيز وعي الأفراد حول حماية معلوماتهم الشخصية على منصات التواصل الاجتماعي،[34] وهو ما سنتناوله في هذا المبحث.

المطلب الأول: الإطار الإجرائي القانوني لجريمة الابتزاز الإلكتروني في التشريع القطري

الفرع الأول: الشكوى في جريمة الابتزاز الإلكتروني

إن مراجعة الشكوى في جريمة الابتزاز الإلكتروني تتطلب فحص مفهوم الشكوى في قانون الإجراءات الجنائية القطري والشروط الإجرائية اللازمة لتقديمها.

(34) ALJI Mohamed and CHOUGDALI Khalid, Digital Investigation of a Cybercrime: Sextortion as a Case Study, Proceedings of the Digital Privacy and Security Conference 2019 10.11228/dpsc.01.01, Electronics and Telecommunication Systems Research Group, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, p: 13

أولاً: مفهوم الشكوى:

عرف بعض الفقهاء الشكوى بأنها تعبير المجني عليه عن إرادته في اتخاذ الإجراءات الجنائية الناشئة عن الجريمة، وهناك رأي آخر في الشكوى مفاده أنها تعبير عن إرادة الضحية يترتب عليه أثر قانوني بموجب اختصاص الدعوى الجنائية كما يتبين من إزالة القيود المفروضة على النيابة العامة فيما يتعلق بالقدرة على تحريك الدعوى الجنائية، والتفسير الأكثر ترجيحًا هو: "البيان الذي أدلى به الضحية أو الضحايا للسلطة المختصة للشكوى رسميا بشأن جريمة ارتكبت ضده أو ضد آخرين، وبالتالي طلب بدء إجراءات جنائية في الحالات التي لا يمكن فيها للنيابة العامة بدء مثل هذا الإجراء دون هذه الشكوى". ويشمل هذا الإجراء بالضرورة تلك الأفعال التي يقوم بها الضحية أو ممثله القانوني والتي توجه إلى ضابط الشرطة القضائية، أو إلى عضو في النيابة العامة، أو محكمة مختصة، بهدف تحريك الإجراءات القانونية اللازمة ضد مرتكب الجريمة المعنية فيما يتعلق بتلك الجرائم التي تم تأسيسها فقط بموجب أحكام قانونية، كما تنص المادة (3) من قانون الإجراءات الجنائية القطري على أنه: "لا يجوز تحريك الدعوى الجنائية إلا بناء على شكوى من المجني عليه أو من يمثله في الجرائم المنصوص عليها في المواد (331)، (330)، (329)، (326)، (325/1)، (323/1)، (309)، (308)، (308)، (293)، (332)، (333)، (357)، (389/1)، (393/1)، (394)، و(395) من قانون العقوبات، وكذلك في الجرائم الأخرى المنصوص عليها في القانون، ويجب أن تقدم الشكوى شفاهة أو كتابة من المجني عليه أو من يمثله قانونًا إلى النيابة العامة أو إلى أحد مأموري الضبط القضائي، وإذا وقعت الجريمة متلبسًا بها وجب تقديم الشكوى إلى من يكون حاضرًا من رجال السلطة العامة".

ثانيًا: ميعاد تقديم الشكوى:

أوجب المشرع القطري تقديم الشكوى خلال مدة محددة؛ حيث تنص المادة (7) من قانون الإجراءات الجنائية القطري على أنه: "لا تقبل الشكوى بعد ثلاثين يومًا من اليوم الذي علم فيه المجني عليه بالجريمة ومرتكبها، أو من اليوم الذي علم فيه من ينوب عنه بها، ما لم ينص القانون على خلاف ذلك". وقد أوضحت محكمة النقض القطرية ما يترتب على هذه المهلة لتقديم الشكوى، وقد قضت المحكمة بأنه: "لا يجوز تقديم الشكوى بعد انقضاء ثلاثين يومًا من علم المجني عليه بوقوع الجريمة وهوية مرتكبها". ويشير هذا النص إلى أن سريان هذه المدة قد نص عليه المشرع قرينة قانونية لا تقبل أي دليل ينفي افتراض التنازل. وقد نص المشرع على أن سكوت المجني عليه في هذا الصدد خلال هذه المدة يعد تنازلاً عن حق الشكوى. وبالتالي، فإذا ظل حق الشكوى قائمًا أو مستمرًا، فلا يجوز استخدامه كأداة للترهيب أو الابتزاز أو الانتقام. وبالمثل، فإن تقديم الشكوى في غضون المدة التي ينص عليها القانون يزيل مجرد افتراض التنازل وينقذ العواقب القانونية لهذا الإجراء.

ثالثًا: مقدم الشكوى:

تقدم الشكوى من المجني عليه أو وكيله القانوني، وفي حالة تعدد المتضررين يكفي أن يتقدم أي منهم بالشكوى، أما في حالة تعدد المتضررين وكانت الشكوى ضد شخص واحد فإنها تعتبر قد قدمت ضد الآخرين جميعًا، ولا بد من الإشارة إلى أنه إذا لم يكمل المتضرر السادسة عشرة من عمره أو كان مصابًا بعاهة عقلية تقدم الشكوى من الشخص الذي له الولاية عليه، أما إذا كان المتضرر شخصًا اعتباريًا تقدم الشكوى من ممثله القانوني أو من يفوضه. وفي هذا الصدد قضت محكمة التمييز القطرية بقولها: "إن الدفوع التي ساقها الطاعن لرفض إسقاط حق المجني عليه في تقديم الشكوى من الميعاد المنصوص عليه في المادة (3) من قانون الإجراءات الجنائية مرفوضة لأن المشرع نص في المادة (3) من قانون الإجراءات الجنائية على أنه لا يجوز تحريك الدعوى الجنائية بناء على شكوى المجني عليه أو من يمثله إلا عن جرائم معينة واردة في قائمة شاملة وليست من الجرائم التي ارتكبها الطاعنون، وبناء على ذلك فإن الدفوع المتعلقة بالشكوى تصبح غير ذات قيمة، ولا يغير من هذا ما ساقه الطاعن الثاني من ضرورة تطبيق القياس في هذه الدعوى؛ إذ يتبين من نص المادة (3) أعلاه أن جميع الجرائم المنصوص عليها في تلك المادة تدخل في نطاق الباب السابع من الكتاب الثاني -الجرائم الاجتماعية- والجرائم الواردة في الكتاب الثالث من قانون العقوبات، والتي لا تتعلق إلا بحقوق فردية خاصة، بحيث يكون لكل منهما أهلية تقديرية للتنازل عن حقوقه".

وفي جميع الأحوال ينتهي حق المجني عليه في الشكوى بوفاته، أما إذا توفي المجني عليه بعد تقديم الشكوى فلا أثر لذلك على استمرار الدعوى، وقد نص المشرع القطري على أن صاحب الشكوى أو الطلب يجوز له التنازل عنها في أي وقت قبل صدور حكم نهائي في الدعوى، والشروط المفروضة على مقدم التنازل هي الشروط نفسها المفروضة على مقدم الشكوى أو الطلب، وهي توافر الشروط المذكورة أعلاه فيما يتعلق بمؤهلات المشتكي وقبوله، أما إذا تعدد المشتكون فلا يكون التنازل ملزمًا إلا إذا وقع عليه جميع المشتكين. ومن الجدير بالذكر أن التنازل الصادر من أحد المتهمين يعتبر تنازلاً من جميع المتهمين، وهذا يعني انتهاء الدعوى الجنائية، أما إذا مات المشتكي فلا ينتقل هذا الحق في التنازل إلى خلفائه، وفي هذا الصدد قضت محكمة التمييز القطرية بأنه: "لما كان من المقرر أن الطلب يختلف اختلافًا جوهريًا عن الشكوى من حيث إنه قرار إداري لا يعتمد على الإدارة الشخصية بل وفقًا لمعايير موضوعية في الدولة ولا يثبت إلا بالكتابة، في حين أن التشابه الوحيد بين الطلب والشكوى هو التنازل عنهما وفقًا للمادة (10) من قانون الإجراءات الجنائية، ونظرًا لهذا الوضع، ولما كان القانون لم يشترط تقديم الطلب خلال مدة معينة

من تاريخ الجريمة -ولم يرد نص في هذا الشأن فيما يتعلق بالشكوى- فإن الحق في تقديمه يستمر إلى أن تصبح الدعوى الجنائية باطلة بعد انقضاء المدة المنصوص عليها في المادة (14) من قانون الإجراءات الجنائية، والاعتراض في هذا الصدد يعد خطأ في تطبيق القانون.

رابعًا: تقديم الشكوى:

في قانون مكافحة الجرائم الإلكترونية أصدر المشرع القطري في القانون رقم (14) لسنة 2014 قانون مكافحة الجرائم الإلكترونية، والذي لم يقيد صراحة حرية النيابة العامة في تحريك الدعوى عن كافة الجرائم المشمولة به، بتقديم شكوى من المجني عليه، كما فعل في بعض الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجنائية، وهذا يعني أن قيد الشكوى لا يسري على الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجنائية إذا ارتكبت عن طريق شبكة الإنترنت؛ أي أنها أصبحت جرائم إلكترونية، وبالتالي يجوز تحريكها من قبل النيابة العامة، ولا يجوز للمجني عليه التنازل عنها، ولذلك قضت محكمة التمييز القطرية بأن: "المادة 3 من قانون الإجراءات الجنائية تنص على أنه: لا يجوز رفع الدعوى الجنائية إلا بناء على شكوى من المجني عليه أو من يمثله في الجرائم المنصوص عليها في قانون العقوبات، وكذلك في الجرائم الأخرى المنصوص عليها في القانون". كما نصت المادة (10) من القانون ذاته على أنه يجوز لمن قدم الشكوى التنازل عنها في أي وقت إلى أن يصدر حكم نهائي في الدعوى، وبالتالي تنقضي الدعوى الجنائية بالتنازل. وحيث إنه يتبين من الأوراق أن الجريمتين اللتين أقامت النيابة العامة من أجلهما المحكوم عليه وأدين من أجلهما معاقب عليهما بمقتضى المادة (89) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية، وقد خلا القانون المذكور صراحةً من تقييد حرية النيابة العامة في تحريك الدعوى عنهما وعن سائر الجرائم الواردة فيهما بمجرد تقديم شكوى من المجني عليه، كما فعل في بعض الجرائم المنصوص عليها في المادة (3) من قانون الإجراءات الجزائية المذكور، والتي لم يقم المحكوم عليه بعقوبة عنها بمقتضى أي منها، وإن ما يثيره المحكوم عليه في هذا الشأن بخصوص تحريك الدعوى أو انقضائها بالتنازل غير مقبول، ولا تكون المحكمة مسؤولة إذا لم تتطرق إلى دفاعه في هذا الشأن، ولو تطرق إليه الحكم المطعون فيه ورفضه على نحو يتفق مع هذا الرأي السابق.

الفرع الثاني: الطبيعة الخاصة للأدلة الإلكترونية وإجراءات ضبطها في جريمة الابتزاز الإلكتروني

أولاً: الطبيعة الخاصة للأدلة الرقمية في جرائم الابتزاز الإلكتروني:

الأدلة الرقمية بما فيها أجهزة الحاسوب والأجهزة الإلكترونية التي تتواجد فيها تلك

الأدلة، أدلة هشة وحساسة لدرجات الحرارة العالية والرطوبة والصدمات الكهربائية والكهرباء الساكنة والمجالات المغناطيسية، وينبغي لمن يقوم بعمليات جمع الأدلة الرقمية باتخاذ الاحتياطات اللازمة عند التوثيق والتصوير والتغليف والنقل والتخزين لتلك الأدلة الرقمية وأجهزتها لتجنب تغيير أو إتلاف أو تدمير البيانات.

كما أن الأدلة الرقمية في جرائم الابتزاز الإلكتروني لها خصائص فريدة تميزها عن الأدلة التقليدية في الجرائم الأخرى، وتفرض مجموعة من التحديات التي يجب معالجتها بعناية خلال التحقيقات. وفي هذا السياق يجب أن تفهم الطبيعة الخاصة لهذه الأدلة من خلال عدة جوانب رئيسة :

1- القابلية للتعديل والتغيير:

الأدلة الرقمية، مثل الرسائل الإلكترونية والصور والفيديوهات والمحادثات على وسائل التواصل الاجتماعي، تتمتع بقدرة عالية على التعديل أو التغيير، فيمكن بسهولة تعديل المحتوى الرقمي أو حذفه، مما يجعل من الضروري توثيق الأدلة وحمايتها فور اكتشافها. ويساهم استخدام تقنيات التجزئة (Hashing) مثل MD5 أو SHA في ضمان سلامة البيانات وعدم تعديلها بعد جمعها.

2- التوقيت الحرج للأدلة الرقمية:

الأدلة الرقمية تتغير بسرعة خصوصًا في الجرائم التي تحدث عبر الإنترنت، فعلى سبيل المثال: قد تختفي رسائل الابتزاز أو يتم تعديل المنشورات والصور في أي لحظة، لذلك يتطلب جمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني سرعة كبيرة واتباع إجراءات قانونية دقيقة لضمان الحفاظ على الأدلة قبل تعديلها أو إخفائها.

3- التوزيع المتعدد للأدلة:

في حالات الابتزاز الإلكتروني، قد تكون الأدلة موزعة عبر منصات متعددة مثل وسائل التواصل الاجتماعي، والبريد الإلكتروني، وتطبيقات المراسلة، مما يجعل من الضروري تحديد جميع المصادر الممكنة للأدلة، واستعمال أدوات متخصصة لجمع هذه البيانات من منصات مختلفة مثل Facebook أو WhatsApp، مع ضمان الحفاظ على توثيق كامل لها.

4- القدرة على استعادة الأدلة المحذوفة:

من أبرز سمات الأدلة الرقمية هي قدرتها على الاستعادة حتى إذا تم حذف البيانات يمكن للأدلة الرقمية أن تسترجع باستخدام تقنيات تحليل البيانات الجنائية، مثل "استعادة الملفات

المحذوفة" باستخدام أدوات مثل EnCase و FTK Imager، هذه الأدوات تمكن المحققين من استرجاع البيانات المحذوفة من الهواتف الذكية أو أجهزة الكمبيوتر.

5- التوثيق والتسلسل الزمني:

الأدلة الرقمية تتطلب توثيقًا دقيقًا لكل خطوة من خطوات جمعها وتغليفها ونقلها، ويجب توثيق توقيت جمع الأدلة، وتوضيح الأدوات المستخدمة في جمع الأدلة وتغليفها، كما أن التسلسل الزمني للأدلة الرقمية يعد أمرًا بالغ الأهمية لإثبات العلاقة بين الجريمة والفاعل.[35]

6- الحفاظ على سلامة الأدلة:

أحد أبرز التحديات في التعامل مع الأدلة الرقمية هو الحفاظ على سلامتها من التلاعب، فعملية نقل الأدلة تتطلب تأمينها وحمايتها باستخدام تقنيات مثل التشفير أثناء النقل والتخزين، وأي تغيير في البيانات يمكن أن يؤدي إلى رفض الأدلة في المحكمة.

والأدلة الرقمية بجميع مصادرها المختلفة متطورة ومتنوعة، كما أن هناك أدلة رقمية يمكن الحصول عليها مباشرة أثناء التواجد في مسرح الجريمة دون الحاجة للنقل والتغليف، والبعض يحتاج إلى النقل، والبعض يحتاج إلى التغليف والنقل والتخزين، وبغض النظر عن نوع الدليل فإن هناك إرشادات بناءً على أفضل الممارسات خاصة بإجراءات تغليف ونقل وتخزين ما تم ضبطه وجمعه من الأدلة الرقمية ومصادرها المختلفة، ويحتاج للتغليف أو النقل أو التخزين أو لهم جميعًا، وينبغي أن يتم تطبيق إجراءات التغليف والنقل والتخزين بطريقة دقيقة وموثوقة؛ لتجنب تغيير أو تدمير أو إتلاف البيانات الرقمية. وعملية التغليف يقصد بها وضع الأجهزة والمكونات التي تحتوي على دليل رقمي داخل أوعية خاصة أو تغليفها بأغلفة خاصة، ولذلك فإنه في هذا السياق نعني بالتغليف أيضًا تعبئة الأجهزة في حاويات أو أكياس خاصة، وفيما يلي سنقوم بذكر الخطوات المهمة التي ينصح باتباعها عند تنفيذ أي من تلك الإجراءات.[36]

(35) Ahmed A. Abd El-Latif, Lo'ai Tawalbeh, Manoranjan Mohanty, Brij B. Gupta, Konstantinos E. Psannis, igital Forensics and Cyber Crime Investigation Recent Advances and Future Directions, 2025, pp: 4346-, https: //www.routledge.com/Digital-Forensics-and-Cyber-Crime-Investigation-Recent-Advances-and-Future-Directions/AbdEl-Latif-Tawalbeh-Mohanty-Gupta-Psannis/p/book/9781032075396

(36) Jeremy Leighton John, Digital Forensics and Preservation, DPC Technology Watch Report 1203- November 2012, Series editors on behalf of the DPC, Published in association with Charles Beagrie Ltd., pp: 915-, https: //www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-reports-1810-/dpctw1203--pdf/file

ثانيًا: إجراءات ضبط الأدلة الرقمية في جرائم الابتزاز الإلكتروني:

لا تختلف جريمة الابتزاز الإلكتروني عن غيرها من الجرائم التقليدية والجرائم الإلكترونية من حيث إجراءات الدعوى المرتبطة بها والمراحل التي تمر بها، وإن كان من الصعب في الجرائم الإلكترونية المرتكبة عن طريق الوسائل الإلكترونية أو شبكة الإنترنت - كما هو الحال في جريمة الابتزاز الإلكتروني- إثبات مسؤولية مرتكبيها. ويتولى مأمورو الضبط القضائي التحقيق في الجرائم والبحث عن مرتكبيها وجمع الأدلة اللازمة للتحقيق والمحاكمة. كما يجوز لمأموري الضبط القضائي الاستعانة بالخبراء في جريمة الابتزاز الإلكتروني، وطلب رأيهم شفاهةً أو كتابة. وقد نصت المادة (63) من القانون القطري رقم (23) لسنة 2004 بإصدار قانون الإجراءات الجنائية على أن: "تجري النيابة العامة التحقيق في الجنايات والجنح التي ترى لزوم التحقيق فيها". ولذلك فإن النيابة العامة – أو من تفوضه من مأموري الضبط القضائي– تقوم بتفتيش الأشخاص والأماكن ونظم المعلومات المتعلقة بالجريمة، على أن يكون أمر التفتيش مسببًا ومحددًا، ويجوز تجديده أكثر من مرة ما دامت مبررات هذا الإجراء قائمة، وإذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل تتعلق بالجريمة، وجب على مأموري الضبط القضائي عرضها على النيابة العامة لاتخاذ اللازم بشأنها. وإن نص المادة (15) من القانون القطري رقم (14) لسنة 2014 بإصدار قانون مكافحة جرائم تقنية المعلومات (14/2014)، المتضمن حظر استبعاد أي دليل ناتج عن وسائل تقنية أو أنظمة معلومات أو شبكات معلومات أو مواقع إلكترونية أو بيانات ومعلومات إلكترونية بسبب طبيعة تلك الأدلة، وتنص المادة (16) على أنه: "لا يجوز استبعاد أي دليل حصلت عليه الجهة المختصة أو جهات التحقيق من دول أخرى لهذا السبب، ما دام قد تم الحصول عليه وفقًا للإجراءات القانونية والقضائية للتعاون الدولي"، يتفقان مع المادة (204) من قانون الإجراءات الجنائية القطري رقم (23) لسنة 2004، التي تنص على أنه: "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه ضروريًا لظهور الحقيقة". وفي جميع الأحوال يجوز للنيابة العامة أن تأمر بجمع الأدلة والتسجيل الفوري لأي بيانات أو معلومات إلكترونية أو بيانات مرور أو معلومات محتوى تراها ضرورية لمصلحة التحقيقات في جريمة الابتزاز.

وللنيابة العامة أن تأمر جميع الجهات ذات العلاقة بتسليم الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو معلومات المحتوى المتعلقة بموضوع الجريمة أو ما يفيد في كشف الحقيقة، كما لها أن تأمر بضبط الأجهزة أو الأدوات أو الوسائل المستخدمة في ارتكاب الجريمة، ولها أن تأمر باتخاذ التدابير والإجراءات الكفيلة بالمحافظة على هذه الأجهزة أو الأدوات أو أنظمة المعلومات أو البيانات أو المعلومات

الإلكترونية، وذلك لحين صدور قرار من الجهات القضائية المختصة بشأنها. وباستثناء الالتزامات المهنية المنصوص عليها في القانون، لا يجوز لأي شخص أن يستند إلى الأسرار المهنية أو متطلباتها للامتناع عن تقديم المعلومات أو الوثائق المطلوبة وفقًا لأحكام هذا القانون.

الفرع الثالث: شروط مشروعية ضبط الدليل الإلكتروني في جريمة الابتزاز الإلكتروني أمام القضاء الجنائي

لقد تبنى المشرع القطري في إثبات الجرائم ما يعرف بنظام الأدلة الحرة أو ما يسمى بالقناعة الذاتية أو الشخصية للقاضي؛ أي أن للقاضي في جريمة الابتزاز الإلكتروني حرية قبول كل ما يشكل قناعته ويبني عليها، وكذلك حرية تقدير قيمة هذا الدليل، ولا يحدد هذا النظام طرقًا أو أدلة معينة للإثبات، بل إن للخصوم الحرية التامة في تقديم الأدلة التي تؤدي إلى قناعة القاضي، ويتمتع القاضي بسلطة واسعة في البحث عن الحقيقة واتباع طرق مختلفة تؤدي إلى تكوين قناعته دون التقيد بأساليب معينة. ولذلك قضت محكمة التمييز القطرية بما يلي: "ومن المقرر أنه وإن كان يكفي أن يشك القاضي في ثبوت التهمة حتى يحكم لصالح المتهم بالبراءة، فإن حد ذلك أن يكون قد فحص الدعوى فحصًا شاملاً ثاقبًا، وأن يكون على علم بأدلتها، وأن يكون حكمه خاليًا من عيوب التعليل. ومن الضروري أيضًا في أصول الفقه أن يؤدي الدليل الذي يستند إليه الحكم إلى النتائج التي استند إليها من دون تعسف في النتيجة أو تعارض مع قاعدة العقل والمنطق. ولما كان الأمر كذلك، فإن الحكم في مبرراته للحكم بالبراءة من التهمة... لم يعرض أقوال شهود الإثبات ويبدي رأيه فيها بما له من سلطة تقديرية في تقدير أقوال الشهود، ورفضها تارة لأسباب لا تتفق مع القانون الصحيح وبتأويل غير صحيح للنصوص التي قدمها للتفسير في ضوء وضوحها وبجهد غير مقبول ينطوي على خلط بين قواعد الإثبات في المواد المدنية والجزائية وتطبيق أحكام الشريعة الإسلامية في غير محلها، وتارة أخرى لأسباب غير مقبولة لا تصلح مبررًا لاستبعاد أقوال هؤلاء الشهود، فإن ما ذكره الحكم على النحو المذكور أساس تبرئته غير سليم، لأنه يشير إلى عدم إحاطة المحكمة الكاملة بالواقعة وأدلتها، مما يؤدي إلى معرفة حقيقة التهمة ومدى ثبوتها بهذه الأدلة، ويكشف عن قيام المحكمة بواجبها في الموازنة بين أدلة الإثبات والنفي، مما يؤدي إلى النتيجة التي توصلت إليها، مما يجعل حكمها محل نظر".[37] ويتضح مما تقدم أن تقدير كفاية الأدلة وتوافر الشروط القانونية فيها في جريمة الابتزاز الإلكتروني من الأمور التي تخضع للسلطة التقديرية للقاضي؛ ولذلك قضت محكمة التمييز القطرية بأن: "المقرر أن المعيار في المحاكمات الجنائية هو اقتناع القاضي بناء على

(37) حكم محكمة التمييز القطرية – تمييز جنائي – الطعن رقم 510/ 2015 – جلسة 15 فبراير 2016م

الأدلة المقدمة إليه بإدانة المتهم أو تبرئته، وأن وزن وتقدير أقوال الشهود متروك لمحكمة الموضوع التي تضعهم في المكانة التي تراها وتقدرهم بالقدر الذي تقتنع به. وكانت المحكمة قد أبدت ثقتها واطمئنانها إلى أقوال شهود الإثبات التي تضمنت ما يؤدي إلى ما استندت إليه. وطبقًا للحكم فإن ذلك لشوته وسلامة حكمها فيما يتعلق بجريمة الاشتراك في تزوير المحررات الرسمية التي أدين بها المستأنفون. ويصبح ما يشكو منه المستأنف في هذا الشأن محل خلاف حول سلطة محكمة الموضوع في تقدير أدلة الدعوى، وهو ما لا يجوز الرجوع إليه لإثارته أمام محكمة التمييز. ولا يتغير ذلك بما ذهب إليه في أسباب طعنه بشأن تجاهل المحكمة لأقوال شهود النفي؛ حيث إنه من المقرر أن للمحكمة تجاهل أقوالهم ما دامت لم تقتنع بها".[38] ويمكن توضيح شروط صحة وحجية الأدلة الإلكترونية في جريمة الابتزاز الإلكتروني أمام المحكمة الجزائية من خلال استعراض ما يسمى بالشرعية الإجرائية في جريمة الابتزاز الإلكتروني، والتي ترتكز على عدد من العناصر تتمثل فيما يلي:

أولًا: يجب أن يكون الدليل في جريمة الابتزاز الإلكتروني مشروعًا؛ أي يجب الحصول عليه بطريقة مشروعة، فلا يجوز استعمال أي وسيلة غير مشروعة للتأثير على المتهم للحصول على اعترافه، ومن الوسائل غير المشروعة سوء المعاملة والتهديد بالإيذاء والإغراء والوعود والترهيب والتأثير النفسي واستعمال المخدرات والكحول والأدوية، ويعتبر باطلاً كل دليل تم الحصول عليه عن طريق التعذيب أو الإكراه أو المساس بالسلامة البدنية أو المعنوية للفرد عن طريق التدخل التعسفي، وقد نص قانون الإجراءات الجزائية القطري على أنه: ".. ولا يجوز له أن يحكم على أي دليل لم يعرض عليه في الجلسة أو تم الحصول عليه بطريقة غير مشروعة...، وأن يكون الإجراء الذي حصل به القاضي على الأدلة متفقا مع الإجراءات المشروعة التي تحترم فيها الحريات وتوفر الضمانات المقررة في القانون".

وفي هذا الصدد قضت محكمة النقض المصرية – بشأن إحدى جرائم الابتزاز الإلكتروني– بما يلي: "لما كان الحكم المطعون فيه قد تبين من وقائع الدعوى، أن المتهم استأجر بارًا في العقار الذي يقيم فيه وحصل على ترخيص بمزاولة نشاط ما يسمى "نت كافيه"، وأبلغه في مجال شبكة المعلومات الدولية والحاسبات الآلية، وتوافرت لديه الرغبة في تهديد النساء وابتزازهن للحصول منهن على ما يريد من أموال أو ممارسات غير أخلاقية عبر الإنترنت بعد تصويرهن في ممارسات غير أخلاقية وهمية، وتهديدهن بإرسال تلك الصور إلى أقاربهن أو بيعها ونشرها على الشبكة المذكورة. ومن أجل ذلك أنشأ موقعين إلكترونيين أحدهما باسمه الحقيقي والآخر باسم وهمي، واستخدم الأخير في التعرف على المجني

(38) حكم محكمة التمييز القطرية – المواد الجنائية – الطعن رقم 116 جلسة 5 ديسمبر 2016م

عليها، وإيهامها بأنه يعمل مدعيًا عامًا وأنه يحبها ويريد الزواج منها، وأنه يريد رؤيتها عارية. وعندما رفضت في البداية بدأ يلح عليها تارة بإغرائها بالزواج وتارة أخرى بالتهديد بعدم الزواج منها حتى استجابت لطلبه ومكنته من رؤيتها عارية تماما وفي ممارسات غير أخلاقية، وذلك بإجبارها على القيام بهذه الوضعيات أمام كاميرا الكمبيوتر الخاصة بها والاتصال بجهاز الكمبيوتر الخاص بالمتهم الذي قام بتصوير هذه المشاهد وتسجيل هذه الصور، ثم بدأ يهددها ويحاول ابتزازها بطلب خمسة آلاف جنيه منها وتهديدها بإرسال تلك الصور لأقاربها أو بيعها لآخرين ونشرها على الإنترنت إذا لم تستجب له، وعندما رفضت في البداية أرسل بعض صورها العارية لشقيقتها التي عرضتها على المجني عليها التي أصابها الرعب والخوف من الفضيحة كونها محامية فأبلغت الإدارة المختصة بوزارة الداخلية، وأكدت التحقيقات صحة الواقعة، وتم استخراج عدد من الرسائل المرسلة للمجني عليها على جهاز الكمبيوتر الخاص بها والتي ثبت أنها مرسلة لها من البريد الإلكتروني للمتهم وتتضمن تهديدات بنشر صورها وطلبات مبالغ مالية. وتنفيذًا لإذن النيابة العامة تم القبض على المتهم وضبط جهاز الحاسب الآلي الخاص به المستخدم في ارتكاب الواقعة بمقر إقامته وتبين أنه يحتوي على صور عارية للمجني عليها، مما يؤكد قيامه بإرسال رسائل تهديد من بريده الإلكتروني وإرسال صور المجني عليها لشقيقتها كما يحتوي على صور وأفلام لفتيات أخريات عاريات مكتوب على كل واحدة منهن اسمها وعنوانها ويحوي محادثات مع المتهم وصحة انتحاله اسمين وادعائه للمجني عليها أنه وكيل نيابة وقد استند الحكم إلى أدلة ثبوت الواقعة على هذا النحو في حق المستأنف والتي استند إليها من أقوال المجني عليها وشقيقتها وضباط الشرطة القضائية والتقارير الفنية التي فحصت الحاسب الآلي، وهو دليل جائز يؤدي إلى ما نص عليه الحكم".[39]

ومن هذا الحكم يتبين ما يلي:

1- أن المتهم استأجر محلًا تجاريًا وحصل على ترخيص بمزاولة نشاط "نت كافيه"، واستغل نشاطه في تهديد وابتزاز النساء للحصول منهن على ما يريد من أموال أو ممارسات غير أخلاقية عبر الإنترنت بعد تصويرهن عاريات في ممارسات غير أخلاقية وهمية وتهديدهن بإرسال تلك الصور إلى ذويهن أو بيعها ونشرها على الشبكة المذكورة، وبذلك تتضح أركان الجريمة.

2- أن الجهات المختصة اعتمدت في إثبات الجريمة على استخراج عدد من الرسائل المرسلة إلى المجني عليها من الجاني على جهاز الكمبيوتر الشخصي الخاص بها، والتي ثبت أنها مرسلة إليها من البريد الإلكتروني للمتهم، تهددها بنشر صورها وطلب مبالغ مالية.

(39) مجموعة أحكام النقض المصرية – الطعن 3981 لسنة 80 قضائية – الصادر بجلسة 17 أكتوبر 2011م -

3- بناءً على إذن صادر من النائب العام المختص تم القبض على المتهم وحصلت الأدلة التالية بالطريق القانوني: تم ضبط جهاز الحاسب الآلي الخاص بالمتهم الذي استعمل في ارتكاب الواقعة بمقر إقامته وتبين أنه يحتوي على صور عارية للمجني عليها، مما يؤكد قيامه بإرسال رسائل تهديد من بريده الإلكتروني وإرسال صور المجني عليها لشقيقتها، كما تبين أنه يحتوي على صور وأفلام لفتيات أخريات عاريات مكتوب على كل واحدة منهن اسمها وعنوانها، إلى جانب محادثات مع المتهم وصحة اتخاذه لاسمين وادعائه للمجني عليها أنه وكيل نيابة.

4- استند حكم الاستئناف إلى ثبوت الواقعة على هذا النحو في حق المستأنف، وذلك بناءً على ما حصل عليه من أدلة من أقوال المجني عليها وشقيقتها وضباط الشرطة القضائية والتقارير الفنية التي فحصت الحاسب الآلي، وهو دليل صحيح يؤدي إلى ما نص عليه الحكم.

ثانيًا: عند تناول جريمة الابتزاز الإلكتروني يراعى مبدأ براءة المتهم، وضرورة إشراف القضاء على الإجراءات كافة باعتباره الحارس الطبيعي للحقوق والحريات، فضلاً عن ضمان حق المتهم في الدفاع عن نفسه ونفي التهمة المنسوبة إليه. وفي هذا الصدد قضت محكمة التمييز القطرية بأنه: "من المقرر أن نفي التهمة وكيدية الاتهام دفاعان موضوعيان لا يستحقان الرد ما دام الرد عليهما مستمدًا من أدلة الإثبات التي استند إليها الحكم. هذا فضلاً عن أن الحكم لكي يثبت ويكون سليمًا يجب عليه أن يورد الأدلة التي قدمها والتي تصح على ما خلص إليه من وقوع الجريمة المنسوبة إلى المتهم، ولا يلزمه أن يلاحقه في كل تفصيل من تفاصيل دفاعه، لأن ما يترتب على تجاهله لها هو رفضه لها، وعليه فإن ما يثيره الطاعن في هذا الشأن لا يعدو أن يكون جدلاً موضوعيًا في تقدير الأدلة وفي سلطة محكمة الموضوع في ترجيح عناصر الدعوى واستنباط اعتقادها، وهو ما لا يجوز إثارته أمام محكمة التمييز."[40]

ثالثًا: تجدر الإشارة إلى أن المشرع القطري قد اشترط في التوقيع الإلكتروني كدليل إثبات أن يتوافر فيه الآتي:

1- أن تكون معلومات إنشاء التوقيع مرتبطة بالموقع وليس بأي شخص آخر.
2- أن تكون معلومات إنشاء التوقيع وقت التوقيع تحت سيطرة الموقع وليس أي شخص آخر.
3- إمكانية اكتشاف أي تغيير يطرأ على التوقيع الإلكتروني بعد حدوث التوقيع.
4- إمكانية اكتشاف أي تغيير يطرأ على معلومات رسالة البيانات بعد وقت التوقيع إذا كان الغرض من اشتراط التوقيع – قانونًا– هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع.

(40) محكمة التمييز القطرية – تمييز جنائي – الطعن رقم 63 لسنة 2017م – جلسة 16 أكتوبر 2017م

المطلب الثاني: القواعد الفنية لجمع الأدلة الرقمية في جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي

الفرع الأول: مرحلة الإعداد وجمع الأدلة من مواقع التواصل الاجتماعي

جمع الأدلة الرقمية من مواقع التواصل الاجتماعي في حالات جرائم الابتزاز الإلكتروني يتطلب خطوات دقيقة ومتخصصة؛ إذ يجب الحفاظ على مصداقية الأدلة وحمايتها من التلاعب لضمان قبولها في المحاكم. وفيما يلي شرح تفصيلي لهذه الخطوات، مع التركيز على ممارسات جمع الأدلة الرقمية من مواقع التواصل الاجتماعي: [41]

أولاً: تحديد نطاق الأدلة المطلوبة وتخطيط عملية الجمع:

- الخطوة الأولى: تحديد الأدلة التي قد تكون متاحة على الحسابات أو الصفحات المتورطة في عملية الابتزاز، وتتضمن هذه الأدلة الرسائل النصية، والصور، ومقاطع الفيديو، والتعليقات، وسجلات النشاط المرتبطة بالابتزاز.
- الخطوة الثانية: التخطيط الشامل، فمن الضروري وضع خطة لجمع الأدلة بناءً على نوع الجريمة وطبيعة الحسابات المتورطة، على سبيل المثال: إذا كان الابتزاز يتضمن صورًا أو تهديدات مباشرة، يجب التركيز على محتوى الرسائل المباشرة وسجلات المحادثات.

ثانيًا: حفظ الأدلة باستخدام تقنيات التصوير الرقمي والتوثيق المباشر:

- التصوير الرقمي: تستخدم تقنية "لقطة الشاشة" أو "تصوير الشاشة" كطريقة أولية لتوثيق الرسائل، والصور، أو غيرها من المحتويات المعروضة على الحسابات المعنية، ويفضل استخدام برامج تصوير متقدمة تتضمن معلومات عن وقت وتاريخ أخذ اللقطة لضمان المصداقية. [42]
- حفظ الروابط والتفاصيل التقنية: يتم تسجيل الروابط الخاصة بالمنشورات أو الرسائل لضمان القدرة على الرجوع إليها لاحقًا، ويتضمن ذلك تسجيل أسماء المستخدمين، ومعرف الحساب (ID)، والتاريخ المحدد لأي تفاعل ذي صلة. [43]

(41) هند نجيب – ضبط الأدلة الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة – المجلة الجنائية القومية – المجلد 61 – العدد 3 – نوفمبر 2016 – ص102 - https: //ncj.journals.ekb.eg/article_208596_34d8c5ea5267de cb20915a2587933a12.pdf

(42) Valentin Gazeau; Khushi Gupta; Min Kyung An, Enhancing Social Media Data Collection for Digital Forensic Investigations: A Web Parser Approach, 2024 International Conference on Computer, Information and Telecommunication Systems (CITS), Girona, Spain, 1719- July 2024, https: //ieeexplore.ieee.org/xpl/conhome/10608004/proceeding , DOI: 10.1109/CITS61189.2024.10607983

(43) د/ إبراهيم الحسيني، جرائم الحاسوب والتحقيقات الرقمية، 2020.

ثالثًا: الحصول على بيانات الاتصال والموقع الجغرافي إذا كانت متاحة:

العديد من شبكات التواصل الاجتماعي تقدم معلومات محدودة حول الموقع الجغرافي أو عنوان الـ IP للمستخدمين، ومع ذلك ففي بعض الحالات يمكن استنتاج بعض البيانات الجغرافية أو التقنية التي تدل على موقع المبتز إذا كانت المنصة تحتفظ بتلك البيانات.

ويمكن للمحققين الاعتماد على هذه البيانات لتحديد موقع المبتز الجغرافي المحتمل أو على الأقل استبعاد بعض المواقع غير المحتملة.[44]

رابعًا: التواصل مع مزودي خدمات التواصل الاجتماعي:

- طلب البيانات الرسمية: يتطلب جمع الأدلة المتعمقة في الجرائم الإلكترونية – مثل الابتزاز– التواصل مع مزودي الخدمة (كمنصات "FaceBook"، و"X"، و"Instagram") لطلب بيانات إضافية، ويتم إرسال طلبات رسمية بموافقة قضائية للحصول على معلومات دقيقة تتضمن سجلات النشاط وسجلات الدخول إذا كانت متاحة.
- الاستجابة للطلبات الطارئة: في الحالات الحرجة يمكن للمحققين إرسال طلبات طارئة للحصول على بيانات في أسرع وقت ممكن، وخاصة إذا كانت هناك حاجة لحماية الضحية.[45]

خامسًا: التحليل الفني للأدلة الرقمية من مواقع التواصل الاجتماعي:

بعد جمع البيانات الأولية يتم تحليلها باستخدام برامج متخصصة مثل أدوات التحليل الجنائي الرقمي، وتشمل هذه التحليلات فحص الرسائل المتبادلة لتحديد نمط التهديدات والضغط المستخدم، وتحديد أي قرائن تدل على هوية المبتز.

ويمكن تحليل الوسائط المتعددة – مثل الصور والفيديوهات – بحثًا عن بيانات تعريفية (Metadata) قد تشير إلى معلومات إضافية حول وقت ومكان تسجيلها.[46]

سادسًا: حفظ النسخ الأصلية للأدلة الرقمية في قواعد بيانات آمنة:

يتم الاحتفاظ بنسخ من الأدلة الرقمية في قواعد بيانات آمنة، ويفضل أن تكون محمية

(44) James R. Lyle, Barbara Guttman, Digital Investigation Techniques: A NIST Scientific Foundation Review, NIST Internal Report, NIST IR 8354, November 2022, pp: 3740-, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

(45) Digital Forensics and Cybercrime Investigations, https: //criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/digital-forensics-and-cybercrime-investigations/

(46) Kausik Maitra , Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation and Evidence Collection, International Journal of Innovation and Applied Studies ISSN 20289324- Vol. 43 No. 2 Aug. 2024, pp. 261271-, Innovative Space of Scientific Research Journals http: //www.ijias.issr-journals.org/,

ببرامج خاصة للحفاظ على النسخ الأصلية دون تعديل، وذلك بهدف استيفاء المعايير القانونية وضمان قبول الأدلة في المحكمة.

وتستخدم برامج مثل برامج تشفير الملفات وخوارزميات "التجزئة" (Hashing) لحماية البيانات وضمان ثباتها.[47]

سابعًا: إعداد تقرير الأدلة الرقمية لعرضه أمام المحكمة:

إعداد تقرير شامل وموثق يصف كل خطوة في جمع الأدلة، بدءًا من جمع الرسائل حتى تحليلها وحفظها، ويتضمن التقرير توثيقًا زمنيًا للأدلة وأي تفاصيل إضافية تم جمعها من المنصات الاجتماعية.

ويعتبر هذا التقرير وثيقة رسمية يتم استخدامها من قبل المحققين والقضاء كمرجع للتأكد من أن الأدلة جمعت وحللت وفق الإجراءات القانونية المعترف بها.[48]

الفرع الثاني: توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي

توثيق مسرح الجريمة عملية مهمة وتعد سجلاً مهمًا في عملية التحقيق، فمن المهم توثيق مسرح الجريمة بدقة بما في ذلك حالة أجهزة الكمبيوتر ووسائط التخزين وأجهزة الشبكة اللاسلكية والهواتف المحمولة والهواتف الذكية والمساعدات الرقمية الشخصية، وغيرها من أجهزة تخزين البيانات ومكونات الوصول إلى شبكة الإنترنت والأجهزة الإلكترونية الأخرى. ونظرًا لتنوع مصادر الأدلة الرقمية في الحجم والشكل والتقنية، يجب ألا يغيب عن إدراك رجل الأمن المختص بتوثيق مسرح الجريمة أن الأدلة الرقمية لا تكون واضحة أو ظاهرة في جهاز الحاسوب أو الأجهزة الأخرى، بل قد توجد مبعثرة في أجهزة متعددة؛ لذا فإن توثيق مسرح الجريمة ينبغي أن يكون مفصلاً باستخدام الفيديو والتصوير الفوتوغرافي وكتابة الملاحظات والرسومات، ليمكن إعادة أو نقل تفاصيل المسرح لاحقًا، كما ينبغي أن يشمل توثيق الأنشطة والعمليات المعروضة على شاشات الأجهزة توثيقًا كاملاً.

ومن خصائص الأدلة الرقمية اتساع مسرحها، ولذلك فإنه في حال امتد مسرح الجريمة إلى مكان أوسع فيجب توثيق المكونات الرئيسة لتقنية الارتباطات (سلكية أو لاسلكية) بين

(47) The Essential Evidence Collection Guide for Websites, Social Media, and Team Collaboration Tools How to Collect and Preserve Evidence on Websites, Social Media Platforms, and Enterprise Social Networks, 2020, pp: 39- https: //f.hubspotusercontent10.net/hubfs/1818760/PDFs/2020%20The%20Essential%20Evidence%20Collection%20Guide%20for%20Websites%20Social%20Media%20and%20Team%20Collaboration%20Tools%20_%20Guidebook.pdf

(48) مجلة التحقيقات الجنائية الرقمية، العدد 4، 2022

أجهزة الحاسوب والأجهزة التقنية الأخرى في جميع مواقع مسرح الجريمة. وعادةً ما يدل وجود مكونات شبكية - سواء من نقاط وصول سلكية أو لاسلكية- على احتمال وجود أدلة إضافية خارج نطاق مسرح الجريمة الرئيسي أو الذي يتم معاينته حاليًا، وفي حال وجود مثل هذه المكونات الشبكية في مسرح الجريمة فيجب توثيقها توثيقًا مفصلاً أيضًا.

وقد يكون هناك بعض الظروف التي قد لا تسمح لرجال الضبط بجمع جميع المكونات أو الأجهزة الإلكترونية في مسرح أو موقع الجريمة، مما يجعل توثيقها ذا أهمية قصوى، وأيضًا إذا كانت هناك قوانين أو محاذير معينة أو أي عوائق أخرى تمنع أو تحول دون تفتيش أو جمع الأجهزة في مسرح الجريمة فيجب على الأقل توثيقها. (49)

توثيق مسرح الجريمة في جرائم الابتزاز عبر مواقع التواصل الاجتماعي يتطلب إجراءات دقيقة تضمن تسجيل جميع الأدلة الرقمية المرتبطة بالجريمة بشكل موثوق، وإليك الخطوات الأساسية لتوثيق هذه الأدلة في مسرح الجريمة الرقمي:

1- التقاط صور أو لقطات شاشة للمحادثات والمحتوى:

أول خطوة في توثيق مسرح الجريمة هي التقاط صور أو لقطات شاشة للمحادثات كافة، والرسائل، والمنشورات، والصور المرتبطة بالابتزاز على مواقع التواصل الاجتماعي، ويفضل أن يتم التقاط لقطات كاملة تتضمن اسم الحساب، وتاريخ ووقت الرسائل، والتفاصيل المرتبطة بالحادث، بحيث يتم عرض المحادثة بشكل كامل ودقيق.

2- توثيق عنوان الإنترنت (URL):

يجب توثيق عنوان URL للصفحات أو المنشورات أو الملفات التي تحتوي على الأدلة، وذلك لتسهيل الوصول إلى المحتوى الأصلي لاحقًا، ويمكن نسخ عنوان URL ولصقه في ملف توثيق خاص بالقضية، مع مراعاة توثيق تاريخ ووقت الدخول إلى كل رابط.

3- تسجيل معلومات المستخدم والأجهزة:

يتم توثيق جميع المعلومات المتاحة حول المستخدمين المتورطين في الجريمة، مثل أسماء الحسابات، وعناوين البريد الإلكتروني، وعناوين IP إن توفرت، ويمكن الحصول على بعض هذه البيانات من إعدادات الحسابات أو طلبها بشكل قانوني من منصة التواصل الاجتماعي في حال كانت مسجلة.

(49) Barbara Guttman, Douglas R. White, Tracy Walraven, Digital Evidence Preservation Considerations for Evidence Handlers, NIST Interagency Report, NIST IR 8387, September 2022, p: 12, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

4- استخدام أدوات التحليل الجنائي الرقمي:

يفضل استخدام أدوات تحليل جنائي متخصصة لتوثيق الأدلة بشكل احترافي، مثل **En-Case** أو**FTK Imager** ، فهذه الأدوات تتيح حفظ البيانات وتوثيقها دون تعديلها، كما تقوم بحساب قيمة التجزئة للأدلة (hash value) ، مما يضمن عدم تعديلها.

5- حفظ النسخ الأصلية ونسخ احتياطية مؤمنة:

من المهم إنشاء نسخة أصلية من الأدلة المحفوظة ونسخة احتياطية على وسائط تخزين مؤمنة، ويفضل أن تكون الوسائط مشفرة وأن توضع في مكان آمن لمنع الوصول غير المصرح به إليها وضمان حماية الأدلة من الفقدان.

6- التوثيق الزمني للأدلة:

يجب أن يتم تسجيل توقيت وتاريخ جميع الأدلة، بما في ذلك وقت التقاط كل لقطة شاشة أو حفظ ملف معين، فالتوثيق الزمني عامل مهم في المحاكمات؛ حيث يظهر تسلسل الأحداث ويعزز من موثوقية الأدلة الرقمية.[50]

7- إعداد تقارير مفصلة وشاملة:

يتم إعداد تقرير شامل يوضح كل خطوة تم اتخاذها في توثيق الأدلة، بما في ذلك الأدوات المستخدمة، وتفاصيل عن الأشخاص الذين قاموا بجمع الأدلة، وأي تعديل قد يحدث على الأدلة الأصلية، ويعد هذا التقرير جزءًا أساسيًا لتقديم الأدلة للمحكمة بطريقة مهنية.[51]

الفرع الثالث: تحليل الأدلة في جرائم الابتزاز الإلكتروني

يستهدف تحليل الأدلة استخلاص الاستنتاجات التي تستند إلى الأدلة التي عثر عليها وتم فحصها، ويتم هنا استخدام مجموعة من التقنيات والأدوات التي سنتحدث عنها لاحقًا، والفحص والتحليل عمليتان مختلفتان، لكن يحدث نوع من الخلط في المسمى، فالفحص يقوم بالمراجعة التقنية للأدلة من خلال تحديد وفحص واستخراج جميع الأدلة المحتملة من جميع وسائط الأدلة الرقمية التي تم جمعها وضبطها، أما التحليل فيتم فيه تحليل جميع البيانات التي أعدت في الخطوات السابقة بشكل مفصل وبناء الاستنتاجات.[52]

(50) د/ سلمان بن على القحطاني – علوم الأدلة الجنائية الرقمية "المفاهيم وطرق المعالجة " في ضوء التطور التقني الحديث" مرجع سابق - ص 147

(51) د/ أحمد لطفي السيد مرعي - الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني، دراسة مقارنة، بحث منشور في مجلة الدراسات القانونية والاقتصادية - كلية الحقوق - جامعة مدينة السادات، المجلد الثامن، العدد الثاني - يونيو 2022، ص 306ص310

(52) د/ سلمان بن على القحطاني – علوم الأدلة الجنائية الرقمية "المفاهيم وطرق المعالجة " في ضوء التطور التقني الحديث" مرجع سابق - ص 160

وعند التحليل، يقوم المحلل بربط جميع النقاط بما فيها ما تم التوصل إليه من نتائج في مرحلة الفحص، ورسم صورة كاملة للمعني بالقضية، وبعد إعداد قائمة بالأدلة الرقمية ذات العلاقة بالقضية، يقوم المحلل بالبحث عن الإجابة عن جميع التساؤلات المتعلقة بجميع بنود قائمة الأدلة الرقمية؛ مثل: من؟ وماذا؟ ومتى؟ وأين؟ وكيف؟ لإيضاح هوية المستخدم أو التطبيق الذي قام بإنشاء أو تحرير أو إرسال كل بند من بنود قائمة الأدلة، وكيفه جاء هذا الدليل أصلاً إلى الوجود، كما أن المحلل يفسر أيضًا أين تم العثور على الدليل، ويشرح لماذا كل هذه المعلومات مهمة، وماذا تعني بالنسبة للقضية المعنية.

ويمكن للمحللين إعطاء قيمة للنتائج التحليلية، وذلك من خلال البحث عن متى حدثت الأشياء، وكذلك بإنتاج الجدول الزمني الذي يعيد بناء مسرح الجريمة بشكل متماسك، ففيما يخص الأدلة الرقمية يحاول المحللون دائمًا شرح وتفسير متى تم إنشاء هذا الدليل والدخول إليه وتعديله واستقباله وإرساله والاطلاع عليه وإطلاقه، كما أنهم يقومون بملاحظة وتفسير سلسلة الأحداث وتدوينها التي حدثت في الوقت نفسه.

كما أن عمليات التحليل التي يمكن أداؤها تشمل على سبيل المثال: الإطار الزمني، والبيانات المخفية، والملفات، والتطبيقات، والملكية، والحيازة، ويمكن شرح هذه العناصر كالتالي:

1- **تحليل الإطار الزمني**: تحليل الإطار (الجدول) الزمني يمكن أن يكون مفيدًا في تحديد متى وقعت الأحداث على نظام الحاسوب مثلًا، والتي يمكن أن تستخدم كجزء من الربط بين استخدام الحاسوب والأفراد في ذلك الوقت من وقوع الأحداث، وهذا يشمل – على سبيل المثال– تحليل البيانات الوصفية للملفات والخاصة بأوقات وتواريخ التحديث والإنشاء والوصول والتحديث، وكذلك تواريخ وأوقات السجلات المخزنة في ملفات تسجيلات الدخول والخروج والأخطاء وغيرها.[53]

2- **تحليل البيانات المخفية**: من المعلوم أنه يمكن إخفاء البيانات داخل الأجهزة الحاسوبية باستخدام طرق عديدة، منها التشفير والضغط أو بتغيير امتداد الملف. وعليه فإن تحليل البيانات المخفية التي تم استخراجها بواسطة عمليات الفحص ستكون مفيدة جدًّا في كشف واستعادة هذه البيانات، التي قد تشير إلى معارف أو ملكيات أو معنى معين، ومن تلك الطرق على سبيل المثال: محاولة فك كلمات المرور أو التشفير أو عمليات الضغط للتمكن من دخول محتوى الملف المحمي أو المخفي بهذه الطرق، وكذلك التأكد من

(53) Albert j.Marcella, jr.doug menendez, cyber forensics "a field manual for collecting ,examining, and preserving evidence of computer crime", second edition , CRC press , 2008,P: 22

صحة امتداد الملف بالأدوات المناسبة، لذلك فإنَّ محاولة التلاعب بامتدادات الملف وتغيير امتداده الصحيح قد يوحي بأن هناك محاولة لإخفائه. (54)

3- **تحليل التطبيقات والملفات:** العديد من التطبيقات البرمجية والملفات التي تم تحديدها واستخراجها قد تحتوي على معلومات ذات صلة بالتحقيق، كما أنها يمكن أن تعطي نظرة ثاقبة على قدرات النظام ومستوى المعرفة لدى المستخدم، ونتائج هذا التحليل قد تشير إلى وجوب اتخاذ خطوات إضافية في مجال عمليات الاستخراج والتحليل، وهي:

أ- فحص محتويات الملف.

ب- تحديد عدد ونوع نظام (أنظمة) التشغيل.

ج- إيجاد الرابط ما بين الملفات والتطبيقات المثبتة على الجهاز.

د- النظر في العلاقات بين الملفات، على سبيل المثال: ربط تاريخ الدخول للإنترنت إلى ذاكرة التخزين المؤقت وملفات البريد الإلكتروني إلى مرفقات البريد الإلكتروني وغيرها.

ه- تحديد أنواع الملفات ذات الامتدادات غير المعروفة لتحديد قيمتها في التحقيق.

و- فحص مواقع تخزين المستخدمين الافتراضية (default user document) للتطبيقات وهيكلة توزيع الملفات (file structure) في القرص الصلب لتحديد إن كان تم تخزين الملفات في المواقع الافتراضية الخاصة بهم أو في مواقع بديلة. (55)

(54) K. Manivannan and V. Ramanan, Conventional Forensic Approach to Computer Crime Detection, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 22780661-,p-ISSN: 22788727-, Volume 22, Issue 3, Ser. I (May - June 2020), P: 43, DOI: 10.97902203014345-0661/ https: //www.researchgate.net/publication/341371489_Conventional_Forensic_Approach_to_Computer_Crime_Detection

(55) MARCUS K. ROGERS, enterprise Incident Response and Digital Evidence Management and Handling, Information Security Management Handbook, Sixth Edition, VOLUME 2pp: 398403-, https: //engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf

النتائج والتوصيات

أولاً: النتائج:

1- تبين من خلال تحليل الأنماط المختلفة لجرائم الابتزاز الإلكتروني وسمات الجناة وخصائص الجريمة أن الجناة يعتمدون بشكل كبير على عنصر المفاجأة للضحية، مع الضغط الشديد على الضحية للاستجابة لرغبات الجناة وعدم السماح لهم بالتفكير أو الاستعانة بآخرين لدعمهم.

2- من خلال دراسة وتحليل خصائص الجريمة والجناة تبين أن الجريمة تتميز بالتأثير الشديد على الضحية؛ حيث إنها قد تؤدي إلى انتحار الضحية أو الإقدام على أفعال خطيرة، أو قد تؤدي إلى آثار اجتماعية خطيرة كانتشار الفاحشة وهدم الروابط الأسرية، بالإضافة إلى آثار اقتصادية خطيرة على قطاع الأعمال عبر ارتكاب أنماط الابتزاز وغيرها من الأنماط التي تمس المؤسسات والشركات والهيئات الحيوية.

3- غالبًا ما يسعى الجناة في هذه الجريمة إلى الحصول على منفعة مالية أو معنوية أو غير أخلاقية، ويعتمدون في استدراج الضحايا على الوقوع تحت سيطرتهم على مواقع التواصل الاجتماعي بشكل كبير؛ حيث يمكنهم استغلال نقاط الضعف الخاصة بالضحايا من خلال دراسة حساباتهم على مواقع التواصل، والنفاذ إليهم من خلال تحليلهم لمحتوى تلك المواقع، وهو ما يتطلب من المستخدمين الحذر الشديد عند التعامل مع الآخرين عبر تلك المواقع.

4- تؤدي الأدلة الرقمية دورًا كبيرًا في إثبات هذه الجريمة، وهو ما يتطلب الحرص على جمع تلك الأدلة والتحفظ عليها وتحليلها وفقًا للقواعد المرعية؛ حتى تعد حجة على الجاني وتوصل المحققين إلى تحييد هوية الجناة وضبطهم.

ثانيًا: التوصيات:

1- يوصي الباحث بعقد الدورات التدريبية للعاملين في مجال إنفاذ القانون في الجرائم الإلكترونية؛ لتطوير معارفهم بشأن الأساليب الإجرامية والأنماط الجديدة من جرائم الابتزاز الإلكتروني والحيل التي يستخدمها الجناة في استدراج ضحاياهم، وفهم كيفية الحفاظ على الأدلة في مسرح الجريمة الرقمي وطبيعته الخاصة.

2- تعزيز القدرات الخاصة بالمعامل الجنائية الرقمية والفاحصين الرقميين في مجال الطب الشرعي الرقمي والمعمل الجنائي، وتطوير معارفهم بشأن أنماط الجرائم التي تستجد حتى يمكنهم فهم الطبيعة المتجددة لمسرح الجريمة الرقمي وكيفية التحفظ على الأدلة الرقمية في جرائم الابتزاز عبر مواقع التواصل الاجتماعي.

3- إيجاد آلية إلكترونية يمكن من خلالها تلقي البلاغات بشكل آلي ودون تدخل بشري ودون طلب بيانات المجني عليهم في جرائم الابتزاز الإلكتروني، وذلك لتشجيع الإبلاغ عن هذه الجرائم، ويمكن من خلالها القيام بالتحقيقات دون تطلب حضورهم أو تواجدهم في جلسات المحاكمة أو الإفصاح عن شخصياته.

4- إبرام اتفاقية مع مزودي خدمات الإنترنت ومواقع ومنصات التواصل الاجتماعي المختلفة؛ لإيجاد آلية تعمل بالذكاء الاصطناعي لرصد عمليات استدراج الضحايا عبر مواقع التواصل الاجتماعي، وحظرهم بمجرد ارتكابهم للأنشطة التي تعد من قبيل الاستدراج للإفصاح عن أسرار أو معلومات سرية أو صور أو غيرها.

5- تعزيز التعاون مع مواقع التواصل الاجتماعي في إطار الاتفاقية الأممية المبرمة مؤخرًا في أغسطس 2024 من الجمعية العامة للأمم المتحدة؛ بشأن مكافحة الإجرام عبر الإنترنت، والعمل على تفعيل بنودها في إطار الحد من جرائم الابتزاز الإلكتروني عبر مواقع التواصل الاجتماعي.

قائمة المراجع

أولاً: المراجع العربية

- أطروحة ماجستير بعنوان: "الابتزاز الإلكتروني للفتاة عبر مواقع التواصل الاجتماعي "الفيسبوك نموذجًا" دراسة مسحية لعينة من طالبات قسم الإعلام والاتصال – جامعة قاصدي مرباح"، تخصص تكنولوجيا الاتصال الجديدة، الجزائر، مقدمة من سمان جويدة، إيمان مردف 2017م، ص23ص25 – https: //jspui/dz.ouargla-univ.dspace/pdf.mardaf-samane/1/14448/123456789/bitstream
- أحمد سبتي أحمد، محمد نعمان عبد النبي، الابتزاز الإلكتروني وأثره في تهديد المجتمع "دراسة فقهية معاصرة"، كانون الثاني 25, 2022، مجلة جامعة تكريت للعلوم الإنسانية، المجلد 1، الجزء الأول (عدد خاص بالمؤتمر) لعام 2022، العدد 29، ص55ص57 – https://jtuh.org/index.php/jtuh/article/view/1740
- باقر غازي حنون، وحسن حماد حميد ، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، مجلة دراسات البصرة، السنة السادسة عشرة، ملحق العدد (42)، كانون الأول 2021، ص54-53.
- جاسم ناصر جاسم المسلماني، التنظيم القانوني لجريمة الابتزاز الإلكتروني في القانون القطري، رسالة مقدمة للحصول على درجة الماجستير في القانون العام، كلية القانون – جامعة قطر ، يناير 2023م، ص9-7.
- هشام رشدي خير الله، إدراك المراهقات لمخاطر الابتزاز الإلكتروني عبر الإنترنت وتأثيره على اتجاهاتهم نحو استخدام تطبيقات التواصل الاجتماعي عبر الهواتف الذكية "دراسة في ضوء مجتمع المخاطر "، المجلة العلمية لبحوث الصحافة، العدد 24، الجزء الأول، يوليو 2022، ص3-1.
- سعيد زيوش، ظاهرة الابتزاز الإلكتروني وأساليب الوقاية منها قراءة سوسيولوجية وآراء نظرية، مجلة العلوم الاجتماعية، العدد 22، 2017م، ص73-70.
- شريفة محمد السويدي، وزيزي مصطفى نوفل، أسباب الابتزاز الإلكتروني والآثار الاجتماعية والنفسية المرتبطة به "دراسة كيفية"، مجلة الآداب، العدد 146، أيلول 2023م، ص618-616
- Doi: https: //doi.org/10.31973/aj.v1i146.4008 https://aladabj.uobaghdad.edu.iq/index.php/aladabjournal/article/view/4008/3583
- هند نجيب، ضبط الأدلة الإلكترونية بين الإجراءات التقليدية والإجراءات الحديثة، المجلة الجنائية القومية، المجلد 61، العدد 3، نوفمبر 2016، ص102
- https://ncj.journals.ekb.eg article___208596___34d8c5ea5267decb20915a2587933a12.pdf

ثانيًا: المراجع الأجنبية:

- "Coercion and Responsibility in Criminal Law: A Study of the Limits of Criminal Liability" by Douglas Husak, Oxford University Press, 2020, pp: 22: 24
- "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality" by Wang, Y., & Stefanone, M. A., New Media & Society, 2022., DOI: 10.1177/14614448211045148
- "The Impact of Self-Disclosure on Social Media on Personal Relationships: A Cross-Cultural Analysis" by Bazarova, N. N., & Choi, Y. H., Journal of Communication, 2020., DOI: 10.1093/joc/jqz052
- Abdullah Al Habsi · Michelle Butler · Andrew Percy, Blackmail and the self-disclosure of sensitive information on social media: Prevalence, victim characteristics and reporting behaviours amongst Omani WhatsApp users", Security Journal, 2023, pp: 250: 252, https: //doi.org/10.1057/s41284-023-00376-3
- Ahmed A. Abd El-Latif, Lo'ai Tawalbeh, Manoranjan Mohanty, Brij B. Gupta, Konstantinos E. Psannis, igital Forensics and Cyber Crime Investigation Recent Advances and Future Directions, 2025, pp: 43-46, https: //www.routledge.com/Digital-Forensics-and-Cyber-Crime-Investigation-Recent-Advances-and-Future-Directions/AbdEl-Latif-Tawalbeh-Mohanty-Gupta-Psannis/p/book/9781032075396
- Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525-540. https: //doi.org/10.1057/s41284-020-00246-2
- Al Habsi, A., Butler, M., Percy, A., & Sezer, S. (2021). Blackmail on social media: What do we know and what remains unknown? Security Journal, 34(3), 525-540. https: //doi.org/10.1057/s41284-020-00246-2
- Albert j.Marcella, jr.doug menendez, cyber forensics “a field manual for collecting ,examining, and preserving evidence of computer crime”, second edition , CRC press , 2008,P: 22
- ALJI Mohamed and CHOUGDALI Khalid, Digital Investigation of a Cybercrime: Sextortion as a Case Study, Proceedings of the Digital Privacy and Security Conference 2019 10.11228/dpsc.01.01, Electronics and Telecommunication Systems Research Group, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco, p: 13

- Authors. Alma Spaniardi, Janki Modi Avari, Teens, Screens, and Social Connection An Evidence-Based Guide to Key Problems and Solutions, 2023, Jenna Margolis and Dinara Amanbekova, Social Media and Cyberbullying, pp: 81: 83, https: //doi.org/10.1007/978-3-031-24804-7
- Barbara Guttman, Douglas R. White, Tracy Walraven, Digital Evidence Preservation Considerations for Evidence Handlers, NIST Interagency Report, NIST IR 8387, September 2022, p: 12, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
- Cybercrime and Digital Forensics: An Introduction" by Thomas J. Holt, Adam M. Bossler, and Kathryn C. Seigfried-Spellar, Routledge, 2017,
- Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats" by Will Gragido, John Pirc, Nicholas Hoffman, & Daniel Molina, Syngress, 2011, pp: 20-22
- Digital Forensics and Cybercrime Investigations, https: //criminal-justice.iresearchnet.com/criminal-justice-process/impact-of-technology/digital-forensics-and-cybercrime-investigations/
- Holt, T.J., & Smirnova, O. (2014). "Exploring the market for cybercrime tools: Characteristics of buyers and sellers in a digital underground economy." Journal of Criminal Justice, 42(1), 27-38, DOI: 10.1016/j.jcrimjus.2013.11.005
- https: //ieeexplore.ieee.org/xpl/conhome/10608004/proceeding , DOI: 10.1109/CITS61189.2024.10607983
- James R. Lyle, Barbara Guttman, Digital Investigation Techniques: A NIST Scientific Foundation Review, NIST Internal Report, NIST IR 8354, November 2022, pp: 37-40, https: //nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf
- Jeremy Leighton John, Digital Forensics and Preservation, DPC Technology Watch Report 12-03 November 2012, Series editors on behalf of the DPC, Published in association with Charles Beagrie Ltd., pp: 9-15, https: //www.dpconline.org/docs/dpc-technology-watch-publications/technology-watch-reports-1/810-dpctw12-03-pdf/file
- K. Manivannan and V. Ramanan, Conventional Forensic Approach to Computer Crime Detection, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 3, Ser. I (May - June 2020), P: 43, DOI: 10.9790/0661-2203014345 https: //www.researchgate.net/publication/341371489_Conventional_Forensic_Approach_to_Computer_Crime_Detection
- Kasmani, M. F., Ismail, R., Sulong, R. S., & Mahamod, Z. (2018). Cyber blackmailer: Modus operandi and preventive measures. International Journal of Cyber Criminology, 12(2), 334-345

- Kausik Maitra , Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation and Evidence Collection, International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 43 No. 2 Aug. 2024, pp. 261-271, Innovative Space of Scientific Research Journals http: //www.ijias.issr-journals.org/,
- Kshetri, N. (2010). "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives." Springer, 2010, pp: 35-37, http: //ndl.ethernet.edu.et/bitstream/123456789/26704/1/50.pdf
- MARCUS K. ROGERS, enterprise Incident Response and Digital Evidence Management and Handling, Information Security Management Handbook, Sixth Edition, VOLUME 2pp: 398-403, https: //engineering.futureuniversity.com/BOOKS%20FOR%20IT/Book%20Information%20Security%20Mangement%206th%20ed.pdf
- Martinez, M., & Anderson, C, "Cyber Extortion: An Emerging Internet-Based Crime", Journal of Cybersecurity, 2021, pp: 126-129
- Nash, M. (2020). "Coercion, Consent, and the Criminal Law: Understanding the Limits of Criminal Liability." Criminal Law Review, 1, 24-39. DOI: 10.2139/ssrn.3563456
- Paganini, P. (2018). "Understanding the motives behind cyber extortion: A deep dive into ransomware attacks." Journal of Information Security and Applications, 43, 23-32, DOI: 10.1016/j.jisa.2018.06.004
- Pemberton, A., Winkel, F.W., & Groenhuijsen, M.S. (2007). "Taking victims seriously in restorative justice: A crime victim and human rights perspective." European Journal of Crime, Criminal Law and Criminal Justice, 218-220.
- Self-Disclosure and Psychological Well-Being in the Age of social media: A Meta-Analysis" by Nguyen, M. H., Bin, Y. S., & Campbell, A., Cyberpsychology, Behaviour, and Social Networking, 2021., DOI: 10.1089/cyber.2020.0329
- The Essential Evidence Collection Guide for Websites, Social Media, and Team Collaboration Tools How to Collect and Preserve Evidence on Websites, Social Media Platforms, and Enterprise Social Networks, 2020, pp: 3-9 https: //f.hubspotusercontent10.net/hubfs/1818760/PDFs/2020%20The%20Essential%20Evidence%20Collection%20Guide%20for%20Websites%20Social%20Media%20and%20Team%20Collaboration%20Tools%20_%20Guidebook.pdf
- Tommy K.H. Chan, Christy M.K. Cheung, Zach W.Y. Lee, Cyberbullying on Social Networking Sites: A Literature Review and Future Research Directions" , Information & Management, Volume 58, Issue 2, March 2021, 103411, pp: 12: 14 https: //www.sciencedirect.com/science/article/pii/S0378720620303499?via%3Dihub

- Utz, S., Muscanell, N., & Khalid, R., "Self-Disclosure on Social Media: The Role of Intrinsic versus Extrinsic Motivations", Computers in Human Behaviour, 2021, pp: 12-14
- Valentin Gazeau; Khushi Gupta; Min Kyung An, Enhancing Social Media Data Collection for Digital Forensic Investigations: A Web Parser Approach, 2024 International Conference on Computer, Information and Telecommunication Systems (CITS), Girona, Spain, 17-19 July 2024,
- Wang, Y., & Stefanone, M. A., "Social Media Self-Disclosure: The Role of Perceived Privacy, Trust, and User Personality", New Media & Society, 2022., pp: 535-541

التحديات الأمنيَّة التي تواجه الأمن البحري في الخليج العربي وتأثيرها وانعكاساتها على حركة الملاحة البحرية

الدكتور / محمد علي محمد أبوشامة
كبير محاضرين علوم بحرية
الإدارة العامة لأمن السواحل والحدود

حافظ عبدالرحمن عبدالله عبدالرحمن
محاضر علوم بحرية أول
الإدارة العامة لأمن السواحل والحدود

التحديات الأمنيَّة التي تواجه الأمن البحري في الخليج العربي وتأثيرها وانعكاساتها على حركة الملاحة البحرية

الدكتور/ محمد علي محمد ابوشامة
كبير محاضرين علوم بحرية
الإدارة العامة لأمن السواحل والحدود

حافظ عبدالرحمن عبدالله عبدالرحمن
محاضر علوم بحرية أول
الإدارة العامة لأمن السواحل والحدود

المُلخَّص

تهدف هذه الدراسة إلى تحليل القضايا والمعوقات التي تواجه الأمن البحريّ في الخليج العربيّ وتأثيرها على حركة الملاحة البحريّة؛ إذ يعد الخليج العربيّ منطقة استراتيجية ذات أهمية بالغة للاقتصاد العالمي بسبب احتوائه على أحد أهم ممرات النقل البحريّ في العالم. وتتناول الدراسة المعوقات الأمنيّة مثل التهديدات الإرهابيّة، والقرصنة، والتوترات السياسية، بالإضافة إلى العقبات التقنية والإداريّة. تُستخدم المنهجيّة الوصفيّة والتحليليّة لاستعراض هذه المعوقات وتأثيراتها على حركة السفن والنقل البحريّ. أهم نتائج الدراسة: التهديدات الأمنيّة الرئيسة تتضمن القرصنة والتوترات السياسية والإرهاب البحريّ وتهريب المخدرات، والتوترات السياسية تزيد من التهديدات الأمنيّة. تؤثر التهديدات والمعوقات الأمنيّة على حركة الملاحة بوضوح ويظهر ذلك في تأخير الشحنات وتغيير المسارات، بالإضافة إلى أن التوترات في خليج عدن وباب المندب تؤثر بشكل كبير على حركة الملاحة في الخليج العربيّ. أهم التوصيات: أولاً، استخدام أنظمة المراقبة والرصد المتقدمة مثل الرادارات والطائرات بدون طيار لمراقبة السفن والمناطق البحريّة الحساسة بهدف مواجهة القرصنة البحريّة. ثانيًا، مواجهة الإرهاب البحريّ بتعزيز التعاون بين الأجهزة الأمنيّة والاستخباراتية لكشف العمليات الإرهابية المحتملة ومنعها. ثالثًا، مواجهة تجارة التهريب بتفعيل التشريعات والقوانين الصارمة ضد المخالفين للقانون والاستخدام الفعال لأجهزة الكشف والرصد والمتابعة. رابعًا، تعزيز التعاون الدولي الإقليمي لتخفيف التوترات السياسية وإنشاء لجان دبلوماسية لحل النزاعات السياسية المؤثرة على الأمن البحريّ.

الكلمات المفتاحية: الأمن البحريّ – المهددات الأمنيّة البحريّة – الخليج العربيّ.

ABSTRACT

The Security Challenges Facing Maritime Security in The Arabian Gulf and Their Impact and Repercussions on Maritime Navigation Trafficw

PHD/Mohamed Ali Mohamed Abu Shama

Senior Lecturer in Marine Sciences - General Administration of Coast and Border Security

Hafez Abdul Rahman Abdullah Abdul Rahman

Senior marine sciences lecturer - General Administration of Coast and Border Security

This study aims to analyze the issues and obstacles facing maritime security in the Arabian Gulf and their impact on maritime navigation, as the Arabian Gulf is considered a strategic region of great importance to the global economy because it contains one of the most important maritime transport routes in the world. The study addresses security challenges such as terrorist threats, piracy, and political tensions, in addition to technical and administrative complications. Descriptive and analytical methodology is used here to review these obstacles and their effects on ship movement and maritime transport. The most important results of the study are: Main security threats include piracy, political tensions, maritime terrorism, and drug smuggling, and political tensions in general increase security threats. These security threats impact shipping traffic which leads to delaying shipments and changing routes. Tensions in the Gulf of Aden and Bab al-Mandab also greatly affect traffic and navigation in the Arabian Gulf. The most important recommendations of the study are: Firstly, confronting maritime piracy by using advanced surveillance and monitoring systems such as radars and drones to monitor ships and sensitive maritime areas. Secondly, confronting maritime terrorism by strengthening cooperation between security and intelligence services to detect and prevent potential terrorist operations. Thirdly, confronting the smuggling trade by activating strict legislation and laws against violators of the law and the effective use of suitable devices of detection, monitoring and following-up with cases. Finally, strengthening regional international cooperation to ease political tensions and establishing diplomatic committees to resolve political disputes affecting maritime security.

Keywords: Maritime Security – Maritime Security Threats – Arabian Gulf.

المقدمة:

تتمثل التحديات والقضايا التي تهدد الأمن البحريّ في مجموعة من الجرائم المتعددة، فالجريمة ظاهرة اجتماعية قديمة ظهرت في جميع المجتمعات الإنسانية بأشكال مختلفة، وتتميز الجرائم البحريّة بنوع من التكيف بين البيئة البحريّة والأشخاص المرتكبين لهذه الجرائم؛ إذ يعتمد ذلك على التوافق البيولوجي بين الفرد والبيئة البحريّة، بالإضافة إلى المهارات الفنية التي يكتسبها لتنفيذ هذه الجرائم. ويتم تصنيف مرتكبي الجرائم البحريّة بناءً على نوعية الجريمة التي تحدث ضمن البيئة البحريّة، وتأثيرها المباشر على الأمن البحريّ المرتبط بحركة النقل البحريّ.

الجرائم البحريّة هي نوع من أنواع الجرائم المنظمة والجريمة المنظمة Organized Crime ترتبط بالجريمة الاحترافية Professional والاتحادات الإجرامية Criminals Confederations، أو التنظيمات الإجرامية Criminal Organizations وتعد من وجهة النظر الاجتماعية الأمنيّة عبارة عن «مشروعات عمل نظمت لأهداف تحقيق الكسب الاقتصادي من خلال نشاطات غير قانونية» [1] وأوضح البعض الآخر «أن الجماعات الإجرامية المنظمة هي تنظيم جماعي ومستمر لأشخاص يستخدمون الإجرام والعنف والفساد من أجل الحصول على المال وأهم خصائص هذه الجماعات الاستمرارية والبناء التنظيمي والإجرام والعنف والعضوية القائمة على الانتماء والولاء والرغبة في الإفساد بهدف السيطرة والربح».

ويُعد الأمن البحريّ في الخليج العربيّ من القضايا الحيوية التي تؤثر بشكل كبير على حركة الملاحة البحريّة والتجارة العالمية؛ نظرًا لموقعها الإستراتيجي واحتوائها على مضيق هرمز الذي يُعد أحد أهم ممرات النقل البحريّ في العالم، تواجه هذه المنطقة تحديات أمنيّة معقدة. تشمل هذه التحديات التهديدات الأمنيّة الإرهاب البحريّ، القرصنة، والتوترات السياسية بين الدول المطلة على الخليج العربيّ. تسعى هذه الدراسة إلى تسليط الضوء على هذه القضايا وتحليل تأثيرها على حركة الملاحة البحريّة في الخليج العربيّ.

مشكلة الدراسة:

تتمحور مشكلة الدراسة حول تحديد وتحليل القضايا والمعوقات التي تؤثر على الأمن البحريّ في الخليج العربيّ، وفهم كيفية تأثير هذه المعوقات على حركة الملاحة البحريّة في هذه المنطقة الحيوية. وتعد منطقة الخليج العربيّ من أكثر المناطق الاستراتيجيّة في العالم لنقل النفط والغاز، بالإضافة إلى التجارة الدولية. ومع ذلك، تواجه هذه المنطقة

(1) أشرف سليمان غبريال، أثر المعلومات على أمن المجتمع البحريّ، دراسة ماجستير، الأكاديمية العربيّة للعلوم والتكنولوجيا والنقل البحريّ، الإسكندرية، 2003م، ص23.

تحديات أمنيّة عديدة تشمل التهديدات الإرهابية، والقرصنة البحريّة، والتوترات السياسية، والعقبات التقنية والإدارية. هذه التحديات تؤثر سلبًا على حركة السفن والنقل البحريّ؛ ما يؤدي إلى اضطرابات في الإمدادات العالمية وزيادة التكاليف الاقتصادية. وتهدف هذه الدراسة إلى الإجابة على الأسئلة التالية :

1. ما القضايا الأمنيّة الرئيسة التي تؤثر على الأمن البحريّ في الخليج العربيّ؟
2. كيف تؤثر هذه القضايا على حركة الملاحة البحريّة والنقل البحريّ في المنطقة؟
3. ما الدور الذي تلعبه التوترات السياسية في تفاقم المشكلات الأمنيّة؟
4. ما التدابير الممكنة لتعزيز الأمن البحريّ وتقليل تأثير هذه المعوقات على حركة الملاحة البحريّة؟

فرضيات الدراسة:

1. هناك تأثير كبير للتهديدات الأمنيّة على حركة الملاحة البحريّة في الخليج العربيّ.
2. تؤدي التوترات السياسية دورًا مؤثرًا في تعطيل الأمن البحريّ في المنطقة.
3. يمكن للتعاون الإقليمي والدولي تعزيز الأمن البحريّ وتقليل المعوقات في حركة الملاحة البحريّة.
4. توجد معوقات تقنية وإدارية تؤثر سلبًا على حركة الملاحة البحريّة في الخليج العربيّ.
5. التوترات الأمنيّة والتهديدات في خليج عدن وباب المندب تؤثر على حركة الملاحة في الخليج العربيّ.

أهداف الدراسة:

1. تحليل القضايا الأمنيّة التي تواجه الخليج العربيّ وتأثيرها على حركة الملاحة البحريّة.
2. استعراض التهديدات الإرهابية والقرصنة وتأثيرها على الأمن البحريّ.
3. تقييم دور التوترات السياسية بين الدول المطلة على الخليج العربيّ في تعطيل حركة الملاحة البحريّة.
4. تقديم توصيات لتحسين الأمن البحريّ وتعزيز حركة الملاحة البحريّة في المنطقة.

أهمية الدراسة:

تبرز أهمية الدراسة من خلال التركيز على منطقة الخليج العربيّ التي تُعد من أهم الممرات البحريّة في العالم بفضل دورها في نقل النفط والغاز والتجارة الدولية، كذلك تسهم في :

1. تعزيز الفهم العام للتحديات الأمنيّة التي تواجه هذه المنطقة الحيوية وتأثيرها على الاقتصاد العالمي.
2. تقديم رؤى حول كيفية معالجة مشكلات الأمن البحريّ، بما يسهم في استقرار الإمدادات النفطية والتجارية الدولية.
3. دعم متخذي القرار في اتخاذ تدابير فعّالة لتحسين الأمن البحريّ، وهو أمر بالغ الأهمية لضمان استمرار التدفق الآمن للتجارة البحريّة في منطقة الخليج.
4. تقليل المخاطر الاقتصادية الناجمة عن الاضطرابات في حركة النقل البحريّ عبر اقتراح حلول وتوصيات مبنية على تحليل علمي ومنهجي.

حدود الدراسة:

1. **الحد الزماني:** تغطي الدراسة الفترة من 2010م إلى 2024م، مع التركيز على الأحداث والتطورات الرئيسية التي أثرت على الأمن البحريّ خلال هذه الفترة.
2. **الحد المكاني:** تركز الدراسة على منطقة الخليج العربيّ، بالإضافة إلى الممرات البحريّة الرئيسة مثل مضيق هرمز وباب المندب باعتبار أن هذا الممر يشهد منذ قرابة العام حوادث بحريّة خطيرة عرقلت حركة التجارة الدولية بسبب ما يجري في قطاع غزة وتأثيره المباشر على حركة الملاحة البحريّة في الخليج العربيّ.

منهجية الدراسة:

1. **المنهج الوصفي:** يستخدم لوصف الوضع الحالي للأمن البحريّ في الخليج العربيّ والمعوقات التي تؤثر عليه.
2. **المنهج التحليلي:** يُستخدم لتحليل تأثير هذه المعوقات على حركة الملاحة البحريّة والنقل البحريّ في المنطقة.
3. الاستبانة والتحليل الكمي لعرض البيانات والنتائج المتعلقة بالتحديات الأمنيّة وأثرها على حركة الملاحة البحريّة في الخليج العربيّ.

الدراسات السابقة:

1. **أشرف كشك، نحو استراتيجيّة متكاملة للأمن البحريّ لدول الخليج العربيّ، دراسة علمية منشورة، مجلة الشؤون العربيّة**، 2021:

تركز الدراسة على تطوير استراتيجيّة شاملة للأمن البحريّ في دول الخليج العربيّ، نظرًا لأهمية هذه المنطقة الجيواستراتيجيّة واعتمادها الكبير على النقل البحريّ، اتبعت الدراسة المنهج الوصفي والمنهج التحليلي. تسلط الدراسة الضوء على التهديدات المتزايدة للأمن البحريّ وتقدم توصيات لتعزيز التعاون الإقليمي والدولي لمواجهة هذه التهديدات.

2. **الزبيدي، عبد الله محمد، أمن المضايق والممرات البحريّة في الخليج العربيّ والبحر الأحمر، دراسة علمية منشورة، دار النشر**، 2022:

تناولت هذه الدراسة أهمية المضايق والممرات البحريّة في منطقتي الخليج العربيّ والبحر الأحمر، وذلك باعتبارهما من أهم المناطق الجيوسياسية والاستراتيجيّة في العالم. يسلط المؤلف الضوء على التحديات الأمنيّة التي تواجه هذه الممرات، والجهود المبذولة من قبل الدول المطلة عليها لضمان أمنها واستقرارها، وتهدف الدراسة إلى تقديم فهم شامل للمخاطر والفرص المرتبطة بأمن المضايق والممرات البحريّة في الخليج العربيّ والبحر الأحمر، واتبعت الدراسة المنهج الوصفي والمنهج التحليلي، واقترحت حلولاً عملية للتحديات الأمنيّة التي تواجهها هذه الممرات الحيوية.

3. **السبيعي، أحمد علي، الإطارات القانونية والسياسات لتعزيز الأمن البحريّ في دول مجلس التعاون الخليجي، الأطلسي كاونسل**، 2023:

تناول هذه الدراسة الإجراءات الأمنيّة المطبقة في الخليج العربيّ وانعكاساتها الاقتصادية على النقل البحريّ، ونظرًا للأهمية الاستراتيجيّة للخليج العربيّ باعتباره طريق نقل بحريّ رئيسًا وضروريًا للاقتصاد العالمي، فإن فهم التوازن بين ضمان الأمن والحفاظ على الكفاءة الاقتصادية أمر بالغ الأهمية. وتستكشف الدراسة مختلف التهديدات الأمنيّة مثل الإرهاب والقرصنة والتوترات السياسية، فضلاً عن التحديات الفنية والإدارية. ومن خلال منهجيات وصفية وتحليلية، يقيم البحث مدى تأثير هذه التدابير الأمنيّة على حركة السفن والنقل البحريّ الشامل. وتهدف الدراسة إلى تقديم رؤى وتوصيات لتعزيز الأمن البحريّ مع التخفيف من الاضطرابات الاقتصادية في المنطقة.

4. **محمد، علي محمد، أثر فشل الدولة على ظاهرة القرصنة البحريّة في منطقة القرن الإفريقي (دراسة حالة دولة الصومال الفترة من 2000م – 2020م)، دراسة علمية منشورة، مجلة جامعة البحر الأحمر**،2023:

تكمن أهمية الدراسة في الربط بين فشل الدولة وما ينتج عنها من انفلات أمني ممثل

في ظاهرة القرصنة البحريّة بمنطقة القرن الإفريقي خلال الفترة 2000م – 2020م مع الأهمية العلمية والإضافة النظرية لظاهرة القرصنة البحريّة باعتبارها من أشد الجرائم خطورة على منطقة القرن الإفريقي والشرق الأوسط، واتبعت الدراسة المنهج الاستقرائي والمنهج الوصفي التحليلي، وأكدت أهم النتائج والإحصاءات أن الصومال تعد دولة فاشلة وذات تأثير قوي ومباشر على تنامي ظاهرة القرصنة البحريّة في القرن الإفريقي، ونسبيًا تعد اليمن وكينيا ذواتي تأثير محدود على تنامي ظاهرة القرصنة البحريّة، وأهم التوصيات فيما يخص تحقيق الأمن البحريّ السوداني ضرورة التنسيق والتعاون بين الأجهزة الأمنيّة والمؤسسات البحريّة ذات الصلة من أجل تعزيز وتطوير فاعلية الأمن البحريّ، وفيما يخص تحقيق الأمن البحريّ الإقليمي التأكيد على دعم ومساندة دول المنطقة المضطربة سياسيًا وأمنيًا واقتصاديًا لكي تخرج من دائرة واسم الدول الفاشلة والمنهارة إلى الدول الفاعلة والمستقرة سياسيًا واقتصاديًا.

5. **Smith, A, Piracy in the Modern World: An Analysis of Maritime Security, Journal of Maritime Studies,**2018, 45(3):

خلصت الدراسة إلى أن القرصنة البحريّة لا تزال تشكل تهديدًا كبيرًا للأمن البحريّ والتجارة الدولية، على الرغم من الجهود المكثفة لمكافحتها، وقد اتبعت الدراسة المنهج التحليلي للإحصاءات والبيانات. أوصت الدراسة بضرورة تعزيز التعاون الدولي وتطوير استراتيجيات شاملة تشمل التدابير الوقائية، وتحسين الظروف الاقتصادية والاجتماعية في المناطق المتضررة، وتعزيز القدرات الأمنيّة للبلدان الساحلية.

الفجوة والاختلافات بين الدراسات السابقة وهذه الدراسة:

1. **دراسة أشرف كشك** (2021):

الموضوع الرئيس: تطوير استراتيجيّة شاملة للأمن البحريّ في دول الخليج العربيّ.

الفجوة: ركزت هذه الدراسة على تطوير استراتيجيات متكاملة للتعاون الإقليمي والدولي لتعزيز الأمن البحريّ، ولكنَّ دراستنا تتجاوز تحليل التهديدات لتشمل تأثير هذه التهديدات بشكل مباشر على حركة الملاحة البحريّة في الخليج العربيّ وتسلط الضوء على تأثير التهديدات على الملاحة بشكل أكثر تحديدًا مقارنة بالتركيز على تطوير الاستراتيجيات الأمنيّة العامة.

2. **دراسة الزبيدي، عبد الله محمد** (2022):

الموضوع الرئيس: أمن المضايق والممرات البحريّة في الخليج العربيّ والبحر الأحمر.

الفجوة: هذه الدراسة تركز على الممرات والمضايق البحريّة وتحديات أمنها في الخليج العربيّ والبحر الأحمر، بينما دراستنا تركز بشكل خاص على منطقة الخليج العربيّ

فقط، مع توضيح تأثير التحديات الأمنيّة على حركة النقل البحريّ. الزبيدي يتناول موضوعًا جغرافيًّا أوسع، في حين أن دراستنا أكثر تحديدًا في نطاقها الجغرافي والموضوعي.

3. **دراسة السبيعي، أحمد علي** (2023):

الموضوع الرئيس: الإجراءات الأمنيّة وتأثيرها الاقتصادي في الخليج العربيّ.

الفجوة: هذه الدراسة تركز بشكل أكبر على انعكاسات الإجراءات الأمنيّة على الاقتصاد البحريّ، بينما دراستنا تتناول تأثير التحديات الأمنيّة بشكل مباشر على حركة الملاحة البحريّة نفسها، بالإضافة إلى أنها تعاملت مع الجوانب الفنية والتشغيلية في النقل البحريّ بشكل أوضح، وليس فقط التأثيرات الاقتصادية.

4. **دراسة محمد، علي محمد** (2023):

الموضوع الرئيسي: تأثير فشل الدولة على ظاهرة القرصنة البحريّة في القرن الإفريقي.

الفجوة: هذه الدراسة تركز على القرصنة البحريّة الناتجة عن فشل الدولة في منطقة القرن الإفريقي، وهو موضوع جغرافي مختلف عن دراستنا التي تركز على منطقة الخليج العربيّ. رغم أن كليهما يتناول القرصنة كتهديد أمني، إلا أن دراستنا هذه أوسع، حيث تشمل تهديدات أخرى مثل الإرهاب والتوترات السياسية وتؤثر على الخليج العربيّ تحديدًا.

5. **دراسة Smith, A** (2018):

الموضوع الرئيس: تحليل القرصنة البحريّة في العالم الحديث.

الفجوة: هذه الدراسة تركز بشكل أساسي على القرصنة البحريّة على المستوى العالمي، وتوصي بتعزيز التعاون الدولي. بينما تشمل دراستنا القرصنة كجزء من التهديدات الأمنيّة، إلا أن نطاقها أضيق جغرافيًا (الخليج العربيّ) وأشمل من حيث أنواع التهديدات الأخرى مثل الإرهاب والتهريب والتوترات السياسية.

6. **الفجوة الأساسية:** دراستنا هذه تقدم معالجة لمجموعة متنوعة من التهديدات الأمنيّة في الخليج العربيّ وتأثيرها المباشر على حركة الملاحة البحريّة، مع التركيز على تحليل العلاقة بين التهديدات والملاحة. في المقابل، تركز معظم الدراسات السابقة على جوانب محددة مثل تطوير استراتيجيات الأمن، أو تأثير فشل الدولة على القرصنة، أو تأثيرات اقتصادية محددة، أو القرصنة البحريّة على نطاق عالمي.

مصادر البيانات:

1. الكتب المتخصصة والبحوث والدراسات العلمية.
2. استبانة الخبراء والمختصين في المجال البحريّ.
3. المواقع الإلكترونية بشبكة الإنترنت.

4. مراجعة الأدبيات السابقة المتعلقة بالأمن البحريّ ومهددات حركة الملاحة البحريّة.
5. التقييم بالمشاركة، حيث يعمل الباحثان في المجال البحريّ لأكثر من عشرين عامًا.

تقسيم الدراسة:

تم تقسيم الدراسة لثلاثة فصول ولمباحث ومطالب كالتالي:

1. **الفصل الأول: تحديات الأمن البحريّ:**
   - المبحث الأول: التحديات والتهديدات الأمنيّة المختلفة.
   - المبحث الثاني: التحليل القانوني للتحديات الأمنيّة.
2. **الفصل الثاني: انعكاسات التحديات الأمنيّة وعلاقتها بحركة الملاحة البحريّة في الخليج العربيّ:**
   - المبحث الأول: حركة الملاحة البحريّة وتأثيرات الأمن البحريّ
   - المبحث الثاني: تأثيرات التحديات الأمنيّة المختلفة على حركة الملاحة البحريّة في الخليج العربيّ
3. **الفصل الثالث: تقييم المخاطر والتحديات وتحليل الاستبانة:**
   - المبحث الأول: تقييم المخاطر والتحديات الأمنيّة في الخليج العربيّ Risk Assessment
   - المبحث الثاني: تحليل الاستبانة وتفسيرها.

الفصل الأول

تحديات الأمن البحريّ

تمهيد:

يعد الأمن البحريّ من القضايا الأساسية التي تؤثر بشكل مباشر على استقرار الدول واقتصادها خاصة في المناطق الحيوية مثل الخليج العربيّ، حيث يشكل الخليج العربيّ مسرحًا استراتيجيًا مهمًا للتجارة الدولية وحركة نقل الطاقة وتمر عبره نسبة كبيرة من إمدادات النفط العالمية والسلع الأساسية، إلا أن هذا الموقع الجغرافي الفريد يعرض المنطقة لتحديات أمنيّة متعددة ومعقدة تهدد حركة الملاحة البحريّة واستقرار الدول المطلة على الخليج. في ظل هذه الأهمية الجيوسياسية تواجه المنطقة مجموعة من التحديات الأمنيّة التي تشمل القرصنة البحريّة، والتهريب، والتوترات السياسية الإقليمية. كما أن الوجود العسكري المكثف للقوى العالمية، وتصاعد التوترات بين بعض دول الخليج والدول المجاورة، يزيد من تعقيد المشهد الأمني البحريّ في المنطقة، بالإضافة إلى ذلك، تسهم التطورات التكنولوجية والعسكرية في ظهور تهديدات جديدة تستهدف البنية التحتية البحريّة؛ ما يفرض تحديات إضافية على الأمن البحريّ، ويستعرض هذا الفصل التحديات

الأمنيّة المختلفة التي تؤثر على الأمن البحريّ في الخليج العربيّ، ورأينا بصفتنا باحثين فيما يخص التحليل القانوني لهذه التحديات والمهددات الأمنيّة لحركة الملاحة البحريّة في الخليج العربيّ، وقد تم تقسيم هذا الفصل كالتالي:

المبحث الأول: التحديات والتهديدات الأمنيّة المختلفة

المبحث الثاني: التحليل القانوني للتحديات الأمنيّة

المبحث الأول
التحديات والتهديدات الأمنيّة المختلفة

تعريف الأمن البحريّ:

تعريف الأمن البحريّ يتضمن حماية الدولة ومناطقها البحريّة وبنيتها التحتية واقتصادها وبيئتها ومجتمعها من الأعمال الضارة التي قد تحدث في البحر أو تنطلق منه، ويشمل هذا المفهوم حماية السفن والموانئ والموارد البحريّة من تهديدات مثل الإرهاب، والقرصنة، والتهريب، والهجرة غير الشرعية، ويعتمد تعريف الأمن البحريّ على إدراك التهديدات المحتملة واتخاذ الإجراءات لمواجهتها، مثل ضمان حرية الملاحة، ومنع الجريمة العابرة للحدود عبر البحار، وحماية البيئة البحريّة.[2]

المطلب الأول: التحديات الأمنية التقليدية في المجال البحري

أولاً: القرصنة Piracy:

تعد القرصنة البحريّة شكلاً من أشكال الجريمة المنظمة وعرفتها البحار منذ استخدام الإنسان لها في نقل التجارة، فقد شكلت الهجمات التي يشنها القراصنة تهديدًا كبيرًا للمجتمع البحريّ في الكثير من المناطق، ونتج عن ذلك فقد للأرواح واحتجاز للرهائن وتأثيرات سلبية واضحة على التجارة العالمية. تنتشر القرصنة في مناطق عدة من المسطحات المائية العالمية، ومن أكثر المناطق تعرضًا للقرصنة البحريّة، مضيق ملقا، الممر المائي بين سنغافورة وإندونيسيا ودول شرق آسيا، وبنجلاديش وبحر الصين، والهند، وبحر العرب وخليج عدن، والصومال وتنزانيا ومدغشقر وقناة موزمبيق، وطريق رأس البحر Cape Sea Outer، وغرب أفريقيا، وشرق أفريقيا، وجنوب أفريقيا، والقرن الإفريقي وأنجولا والساحل الغربي وخليج عدن (شرق عدن)، والبرازيل، وجنوب أمريكا. وتُعرّف القرصنة

(2) Natalie Klein, Joanna Mossop, (2) Donald R. Rothwell, Maritime Security: International Law and Policy Perspectives from Australia and New Zealand, Routledge, Taylor & Francis Group, 2010, 21.

وفقًا لاتفاقية الأمم المتحدة لقانون البحار (المادة 101) كما يلي: أي عمل غير قانوني من أعمال العنف والاحتجاز أو السلب يرتكب لأغراض خاصة من قبل طاقم أو ركاب سفينة خاصة أو طائرة خاصة ويكون موجهًا ضد: [3]

1. سفينة أو طائرة أخرى في أعالي البحار أو ضد أشخاص أو ممتلكات على ظهر تلك السفينة أو الطائرة.
2. سفينة أو طائرة أو أشخاص أو ممتلكات في مكان يقع خارج ولاية أي دولة.
3. أي عمل من أعمال الاشتراك التطوعي في تشغيل سفينة أو طائرة مع العلم بوقائع أو «حقائق» تكسب تلك السفينة أو الطائرة صفة القرصنة.
4. أي عمل ينطوي على التحريض على ارتكاب أحد هذه الأعمال الموصوفة في الفقرتين الفرعيتين الأولى والثانية من هذه المادة أو يستهدف عن عمد تسهيل ارتكابها.

نصت المادة (102) من اتفاقية قانون البحار على أنه «إذا ارتكبت أعمال القرصنة المعرفة في المادة (102) سفينة حربية أو سفينة حكومية أو طائرة حكومية تمرد طاقمها، أو استولى على زمام السفينة أو الطائرة اعتبرت هذه الأعمال في حكم الأعمال التي ترتكبها سفينة أو طائرة خاصة. لا يجوز حسب المادة (107) من اتفاقية قانون البحار» أن تنفذ عملية الضبط بسبب القرصنة إلا سفن حربية أو طائرات عسكرية أو غيرها من السفن والطائرات التي تحمل علامات واضحة تدل على أنها في خدمة حكومية ومأذون لها بذلك».

إن القرصنة أعمال ترتكب في أعالي البحار، أما السطو المسلح فيرتكب في المياه الإقليمية، والتي يحق للسفن المرور البريء، أو المرور العابر في المضايق أو القنوات البحريّة، وأثناء المرور البريء أو المرور العابر يظل الاختصاص منعقدًا لدولة العلم الذي تحمله السفينة، فإذا وقع اعتداء على ظهر السفينة أو سيطر ركابها عليها أثناء المرور أو العبور فلا تستطيع الدولة صاحبة السيادة التدخل؛ لأن الاختصاص ما زال معقودًا لعلم السفينة، وقد لا ترغب في التدخل أصلاً، وفي الوقت ذاته لا تستطيع أي دولة أخرى فرض ولايتها؛ لأن الفعل لم يرتكب في أعالي البحار.

جهود المجتمع الدولي لمكافحة القرصنة البحريّة:

1. جهود المكتب البحريّ الدولي (International Maritime Bureau(IMB: تأسس عام 1981م وهو قسم متخصص من غرفة التجارة الدولية (International Chamber of Commerce (ICC،

(3) US Department of Energy, Annual Energy Review. Retrieved from DOE, report, 2020.
الرابط الإلكتروني: https://www.energy.gov

وقد أصدرت المنظمة البحريّة الدولية قرارين11 (A.504(X)–5and9)، والتي تحث فيهما الحكومات والهيئات المعنية بالتعاون وتبادل المعلومات مع المكتب البحريّ الدولي (IMB). يبذل مكتب الملاحة الدولية (IBM) جهدًا في مكافحة القرصنة باعتبارها خطرًا يهدد المصالح التجارية للدول الأعضاء في غرفة التجارة الدولية (ICC).[4]

2. مركز تقارير القرصنة: من الجهود المبذولة تحت رعاية المكتب البحريّ الدولي (IMB) قيامه بإنشاء مركز تابع له في عام1992، ويقع في كوالالمبور بماليزيا تكون مهمته تلقي التقارير، ويقوم هذا المركز بإصدار تقارير دورية أسبوعية، وشهرية، وربع سنوية، وسنوية عن حالات القرصنة أو التهديد بالهجمات أو السطو المسلح على السفن بإذاعتها عن طريق الأقمار الاصطناعية INMARSAT–C وتقدم هذه الخدمات مجانًا لجميع السفن بغض النظر عن موقعها، أو مالكها، أو العلم الذي ترفعه كما يقوم المركز بإصدار تحذيرات حول النقاط الساخنة.[5]

3. غرفة الملاحة الدولية: تمثل هذه الغرفة وجهة نظر صناعة النقل البحريّ ومن عدة قطاعات، ومن عدة دول وعضوية هذه الغرفة تشتمل على هيئات ملاك السفن الوطنية، ومشغلي سفن ناقلات الصب، وناقلات البترول وسفن الركاب، وسفن الحاويات ذات الخطوط المنتظمة. وتهدف غرفة الملاحة البحريّة (ICS) إلى الحفاظ على قدر معقول من النظم الدولية لحسن تسير وإدارة السفن على مستوى العالم بطريقة آمنة وفعالة، وقد أصدرت (ICS) دليلًا عن أماكن حدوث هجمات القرصنة والسطو المسلح وكيفية منعها ومكافحتها.[6]

4. جهود مجلس الأمن الدولي: يبذل مجلس الأمن الدولي (United Nation Security (UNSC Council جهودًا لقمع القرصنة، وأفعال العنف المسلح في البحر، بموجب المادة (34) من ميثاق الأمم المتحدة التي تفوض إليه سلطات حفظ الأمن والسلام الدوليين وإعادتهما إلى نصابهما في حال انتهاكهما، وبهذا فإن القرصنة والسطو المسلح في البحار هي من الحالات التي تهدد الأمن والسلم الدوليين, وبناء على قرار مجلس الأمن الدولي رقم (1851) لعام 2008م أُنشئت مجموعة الاتصالات الدولية بشأن القرصنة في سواحل الصومال (CGPCS) Contact Group on Piracy off the Coast of Somalia وتكونت المجموعة من (24) دولة و(5) منظمات حكومية إقليمية ودولية.

جهود المنظمة البحريّة الدولية (IMO): منذ مطلع عام 1995م أعدت المنظمة البحريّة الدولية برنامجًا لمكافحة القرصنة يتضمن تدابير متعددة الأطراف بقصد تحسين أساليب

(4) https://www.icc-ccs.org/2024.

(5) المرجع نفسه https://www.icc-ccs.org/2024

(6) piracy and armed Robbers: Master Guide,www.marisec.org /piracy, 92008/.

آلية التعاون الدولي لإدارة أمن البحار والموانئ لمواجهة أفعال القرصنة، وبالأخص في المياه بالقرب من القرن الإفريقي، وخليج عدن، وغرب المحيط الهندي، كل ذلك بناء على قرار مجلس الأمن الدولي رقم (1851) للعام 2008م، بشأن القرصنة في سواحل الصومال. دعمت المنظمة البحريّة الدولية المؤتمر الإقليمي بشأن القرصنة البحريّة في يناير 2009م فشارك في المؤتمر ممثلو (17) دولة، وأقر المؤتمر مدونة جيبوتي لمكافحة القرصنة، بشأن قمع القرصنة وهجمات السطو المسلح ضد السفن في غرب المحيط الهندي، وخليج عدن، فيما صدقت على المدونة (9) دول، وينبغي على كل مشارك في هذه المدونة أن يعين جهة اتصال وتنسيق وطنية لتيسير تشاطر المعلومات بطريقة منسقة وسريعة وفعالة بين المشاركين بما يتفق والغرض من هذه المدونة.[7]

ثانيًا: الإطار القانوني للمتسللين (المسافرون خلسة):

يتم التعاون بين كلٍ من الربان وهيئات الموانئ والإدارات الوطنية وباقي الجهات المعنية الأخرى المختصة والعاملين في المجال الأمني من أجل منع الوصول غير الشرعي للمتسللين إلى السفينة. وقد تم تحديد إطار وتدابير دولية معاصرة للمتسللين تدعو في الوقت الراهن إلى التخلص من القلق الذي يلاحق ربابنة السفن، والتي تعد من القضايا المعاصرة للأمن البحريّ، وتعد من القضايا المعقدة للغاية، ويرجع ذلك إلى اختلاف التشريعات الوطنية في كل البلدان المعنية مثل: بلد المغادرة، وبلد النزول أو الوصول، ودولة علم السفينة أو المطالب الفعلية للجنسية والمواطنة للمتسللين وبلدان العبور أثناء العودة إلى الوطن. فقد وضحت المنظمة البحريّة الدولية (IMO)، وفي حالة عدم وجود الإجراءات المتفق عليها دوليًا في التعامل مع المتسللين توجد مصاعب جمة تواجه ربابنة السفن وشركات النقل البحريّ، ولذلك اعتمدت الجمعية العامة للمنظمة البحريّة الدولية القرار رقم (20) (871) عن المبادئ التوجيهية بشأن تخصيص مسؤوليات البحث عن وضع ناجح لحالات المتسللين.[8] الملحق رقم (1) يوضح المبادئ الأساسية التي تنفذ في حالات التسلل.

ثالثًا: الإرهاب البحريّ Maritime Terrorism:

الإرهاب البحريّ يُشير إلى الأنشطة الإرهابية التي تستهدف السفن أو الموانئ أو المنشآت البحريّة بقصد إلحاق الأذى أو تعطيل التجارة البحريّة العالمية. هذه الظاهرة قديمة ولكنها أخذت أبعادًا جديدة مع تنامي حركة التجارة عبر البحار. تشمل الأنشطة الإرهابية البحريّة القرصنة، الهجمات على السفن التجارية والنفطية، خطف الرهائن، والتفجيرات البحريّة. تعد

(7) Djibouti Code of Conduct, 299 ,2009/1/.
الرابط الإلكتروني: https://www.imo.org/en/OurWork/Security/Pages/DCoC.aspx

(8) غبريال، أشرف، 2003، مرجع سابق، 34.

المناطق ذات النزاعات أو تلك التي تعاني من ضعف أمني مثل خليج عدن ومضيق ملقا من أكثر المناطق عرضة للإرهاب البحريّ. هذه الهجمات تُعطّل التجارة العالمية، وتُعرّض حياة البحارة للخطر، وتزيد من تكاليف الشحن والتأمين. وتُسجّل الهجمات البحريّة تزايدًا في السنوات الأخيرة، خاصة في المناطق الساحلية للدول الفقيرة والنامية.[9]

رابعًا: التهريب Smuggling:

يعد التهريب عبر المنافذ البحريّة أصعب وأخطر أنواع التهريب؛ إذ يستعمل المهربون القوارب والسفن البحريّة بقصد تهريب المواد المحظورة من مكان لآخر ومن دولة لأخرى ويعد تجارة غير مشروعة ونشاطًا إجراميًا دوليًا منظمًا يكون الغرض من التهريب هو مخالفة القوانين واللوائح والقواعد الصادرة من السلطات المختصة في الإقليم المعني، بدون الحصول على الموافقة أو الإذن من تلك السلطات، أو لتجنب دفع الرسوم المستحقة وفقًا لما هو محدد في القوانين واللوائح ذات الصلة. يهدف التهريب إلى تحقيق منفعة شخصية أو للإضرار بالمجتمع الإقليمي على الصعيد الاجتماعي أو السياسي أو الديني أو الاقتصادي، ويشمل ذلك:[10]

1. المواد المخدرة: تمثل هذه الأنشطة الإجرامية لتهريب المخدرات خسارة كبيرة جدًا لملاك السفن التي تستخدم سفنهم في التهريب، وعادة ما تجلب المخدرات على ظهر السفن بواسطة وسائل عديدة مثل الأمتعة ومخزونات السفن، أو بواسطة تهريبها في أجسام الأشخاص أو في الأجهزة الإلكترونية.
2. الأسلحة التقليدية: تهريب الأسلحة عادة ما يأخذ نفس القدر من الأهمية للمهربين مثل المخدرات وعادة ما يتم تهريب الأسلحة في الحاويات.
3. المواد المتفجرة.
4. الأسلحة الكيمائية / البيولوجية.
5. المواد أو النفايات المشعة.
6. مواد يحظر دخولها لإقليم الدولة طبقًا إلى اللوائح والقوانين الصادرة في الدولة.
7. تهريب البضائع: غالبًا ما تمثل هذه الجريمة كارثة كبرى لصناعة النقل البحريّ، وتشكل خسارة مالية كبيرة للملاك والوقاية هي أفضل طريقة فعالة للتعامل مع هذه الجريمة والتهديد الأمني المتعلق بها. وعلى الرغم من عدم وجود استخدام عمق أو السعي للحصول على مكاسب من هذه الجريمة، لكنها تبقى ذات تأثير كبير وعلى درجة عالية من الخطورة في قائمة التهديدات الأمنيّة المختلفة.

(9) International Maritime Bureau (IMB). (2023). «Piracy and Armed Robbery Against Ships Annual Report الموقع الرسمي للمكتب البحريّ الدولي/https://icc-ccs.org»

(10) بن عيسى حياة، التهديدات البحريّة الراهنة وجهود مكافحتها، المجلة الجزائرية للقانون البحريّ والنقل، ع 1 (2014)، 137.

خامسًا: التوترات السياسية والنزاعات الإقليمية:

تشكل التوترات السياسية والنزاعات الإقليمية في الخليج العربيّ تحديًا كبيرًا للأمن البحريّ في المنطقة، وذلك نظرًا لتأثيراتها العميقة والمتعددة الأبعاد على استقرار الملاحة البحريّة والتجارة الدولية. من أبرز تأثيرات هذه التوترات: [11]

1. التأثير على أسعار النفط والغاز: النزاعات السياسية في الخليج العربيّ تؤثر بشكل مباشر على أسعار النفط العالمية، نظرًا لأهمية المنطقة كمصدر رئيس للطاقة. وأي تهديد للأمن البحريّ يمكن أن يؤدي إلى ارتفاع أسعار النفط نتيجة لزيادة المخاطر المتعلقة بإمدادات الطاقة.
2. عرقلة التعاون الإقليمي: التوترات السياسية تعيق التعاون بين دول الخليج في مجال الأمن البحريّ، والتباينات السياسية والمصالح المتضاربة تجعل من الصعب تنسيق الجهود الأمنيّة المشتركة لمواجهة التهديدات البحريّة مثل القرصنة والتهريب.

المطلب الثاني: التحديات التقنية والبيئية للأمن البحري

أولًا: المعوقات التقنية والإدارية للأمن البحريّ في الخليج العربيّ:

تواجه الأمن البحريّ في الخليج العربيّ عدة معوقات تقنية وإدارية تؤثر على فعاليته وقدرته على مواجهة التهديدات. من بين هذه المعوقات: [12]

1. العقبات التقنية:

- ضعف البنية التحتية البحريّة: تعاني بعض دول الخليج من نقص في البنية التحتية البحريّة المتطورة، مثل الموانئ الحديثة ومرافق الصيانة للسفن. هذا النقص يحد من القدرة على مراقبة وحماية السواحل البحريّة بشكل فعال، ويؤثر سلبًا على سرعة الاستجابة للحوادث والتهديدات البحريّة.
- التحديات التكنولوجية: تفتقر بعض دول الخليج إلى التكنولوجيا المتقدمة اللازمة لمراقبة وتحليل الأنشطة البحريّة بشكل مستمر. يتضمن ذلك نقص أنظمة الرادار المتطورة، والطائرات بدون طيار، وأنظمة الاتصالات الفعالة التي تسهم في تعزيز الوعي بالمجال البحريّ والتنسيق بين الجهات المختلفة.

(11) Khalid, I, Maritime Security in the Gulf Region, Naval War College Review, 65(4) (2012), 7290-
اسم الموقع: U.S. Naval War College Digital Commons

(12) Katzman, K. The Persian Gulf States and Iran: Issues for U.S. Policy, Congressional Research Service, 814-5 ,2016/.

2. العقبات الإدارية:

- التشريعات والقوانين: تشكل التشريعات والقوانين غير الموحدة بين دول الخليج عائقًا كبيرًا أمام التعاون الإقليمي في مجال الأمن البحريّ. التباين في القوانين والتشريعات البحريّة يعيق جهود التنسيق والتعاون المشترك بين الدول لمواجهة التهديدات البحريّة، الملحق رقم (2) يوضح الاتفاقيات والمعاهدات الإقليمية والدولية.

- الفساد الإداري وتأثيره على الأمن البحريّ: يُعد الفساد الإداري أحد أكبر التحديات التي تواجه الأمن البحريّ في الخليج العربيّ. يؤثر الفساد على تخصيص الموارد بشكل فعال، ويعطل تنفيذ السياسات الأمنيّة اللازمة؛ ما يضعف الجهود المبذولة لمكافحة الأنشطة غير القانونية في المياه الإقليمية.

ثانيًا: الحوادث البحريّة:

تُعد الحوادث البحريّة في الخليج العربيّ من القضايا التي تمثل تحديات كبيرة على حركة الملاحة البحريّة في المنطقة. يتسم الخليج العربيّ بأهمية استراتيجيّة واقتصادية كبيرة، حيث يمر من خلاله جزء كبير من التجارة العالمية وإمدادات النفط. ومع ذلك، فإن تكرار الحوادث البحريّة مثل التصادمات، وتسربات النفط، والانفجارات، يفرض تحديات كبيرة على الأمن البحريّ وعلى حركة السفن. تصادمات السفن وتسربات النفط تترك آثارًا بيئية واقتصادية وخيمة. على سبيل المثال، حادثة تسرب النفط الشهيرة التي وقعت في عام 1991م خلال حرب الخليج أثرت على البيئة البحريّة بشكل كارثي وأدت إلى تدمير الشعاب المرجانية وقتل الحياة البحريّة[13]؛ ما أثر سلبًا على الصيد والسياحة البحريّة. بالإضافة إلى ذلك، فإن حوادث التصادم البحريّ تؤدي إلى تأخير الشحنات وزيادة تكاليف التأمين؛ ما ينعكس سلبًا على اقتصاديات الدول المطلة على الخليج.

ثالثًا: التلوث البحريّ:

يمثل التلوث البحريّ أهم الجوانب السلبية للنهضة الصناعية في القرن العشرين وأصبح يهدد البيئة البحريّة تهديدًا خطيرًا؛ نظرًا لتزايد معدلاته يومًا بعد يوم في معظم بحار العالم خاصة المغلق منها أو الشبه مغلق (مثال للبحار الشبه مغلقة: البحر الأحمر والخليج العربيّ)، كنتيجة مباشرة لما تستقبله تلك البحار من ملوثات بفعل الأنشطة البشرية، أو بفعل العوامل الطبيعية المرتبطة بالبيئة البحريّة.[14]

(13) ويكبيديا، الموسوعة الحرة، تسرب النفط في حرب الخليج الثانية، 2024/8، الساعة 0800.

(15) محمد علي محمد، التلوث البحريّ أسبابه وآثاره وطرق مكافحته، رسالة ماجستير، الأكاديمية العسكرية العليا، كلية القيادة والأركان، اليمن، 2012، ص4.

أحد مفاهيم وتعاريف التلوث البحريّ هو إدخال مواد بطريقة مباشرة أو غير مباشرة إلى البيئة البحريّة نتيجة للأنشطة البشرية المختلفة تؤدي إلى تأثيرات على صحة الإنسان وإعاقة الأنشطة البحريّة المختلفة بما فيها الصيد، وأيضًا تغيير في خواص مياه البحر؛ ما يفقدها صلاحيتها للاستخدام في الأغراض المختلفة.[15] وتعريف آخر عن التلوث البحريّ: لغة هو تلوث مادي ينتج عن اختلاط أي شيء غريب عن مكونات المادة بمادة أخرى، واصطلاحًا هو قيام الإنسان بطريق مباشر أو غير مباشر بالإضرار بالبيئة الطبيعية والكائنات الحية.[16]

رابعًا: الصيد الجائر:

الصيد غير المسؤول أو الصيد الجائر هو زيادة قدرات الصيد (عدد القوارب، أو معدات الصيد، أو الوقت المخصص للصيد) الموجهة نحو استغلال المخزون السمكي بشكل أكبر من تلك القدرة اللازمة لصيد الكميات الزائدة من المخزون، وهو الأمر الذي سيترتب عليه في المستقبل تناقص أعداد الأسماك في هذا المخزون بشكل يؤثر سلبًا على قدرته على تجديد نفسه طبيعيًا؛ ما يؤدي في النهاية إلى ما يسمى بالصيد الجائر، ويترتب عليه انقراض للكائنات البحريّة، واختلال للتوازن البيئي[17].

خامسًا: التغيرات المناخية والظروف الجوية القاسية:

تشهد منطقة الخليج العربيّ تأثيرات متزايدة للتغيرات المناخية، بما في ذلك ارتفاع درجات الحرارة، وندرة المياه، والظروف الجوية القاسية مثل العواصف الرملية وأحيانًا الأمطار الغزيرة، وتؤثر هذه التغيرات بشكل كبير على الحياة اليومية والأنشطة الاقتصادية في المنطقة، وتتمثل تأثيرات التغيرات المناخية والظروف الجوية القاسية في التالي: [18]

1. ارتفاع درجات الحرارة: تشهد منطقة الخليج العربيّ ارتفاعًا ملحوظًا في درجات الحرارة؛ ما يؤثر على العمليات البحريّة والأنشطة الاقتصادية المرتبطة بها.
2. ارتفاع مستوى سطح البحر: يعد ارتفاع مستوى سطح البحر نتيجة مباشرة لذوبان الجليد

(15) محمد السيد أحمد، المسؤولية المدنية عن أضرار التلوث بالزيت، الإسكندرية، دار الجامعة الجديدة، الطبعة الثانية، 2005م، ص35.

(16) محمد أمين عامر، تلوث البيئة، دراسة علمية، القاهرة، دار الكتاب الحديث، 2003، ص204.

(17) https://marocbleu.com/The impact of overfishing on fish wealth, 122018/.

(18) متابعة ذاتية لنشرات الأرصاد الجوية، المستلمة يوميًا من منظومة درع الوطن، منذ 2019 – 2024.

القطبي والتوسع الحراري للمياه نتيجة ارتفاع درجات الحرارة، ويشكل هذا الارتفاع تهديدًا مباشرًا للموانئ والبنية التحتية الساحلية في دول الخليج العربيّ؛ ما يتطلب استثمارات كبيرة في البنية التحتية لمواجهة هذه التحديات.

3. تكرار الظواهر الجوية القاسية: تشهد منطقة الخليج العربيّ زيادة في تكرار وشدة الظواهر الجوية القاسية مثل العواصف الرملية والأمطار الغزيرة؛ ما يؤدي إلى اضطراب حركة الملاحة البحريّة وتأثيرات سلبية على السفن والبنية التحتية البحريّة.

أمثلة على الظروف الجوية القاسية وتأثيرها على الملاحة البحريّة:

1. عاصفة الغبار في السعودية: في مارس 2009، شهدت السعودية واحدة من أشد العواصف الرملية في تاريخها، فقد غطت العاصفة معظم المناطق الشرقية والوسطى من البلاد؛ ما أدى إلى توقف حركة المرور والطيران، وقد تأثرت حركة الملاحة البحريّة بشكل كبير بسبب انخفاض الرؤية وتعطل العمليات في الموانئ؛ ما أدى إلى تأخير الشحنات وتوقف عمليات التفريغ.[19]
2. فيضانات جدة: تعرضت مدينة جدة في السعودية لفيضانات شديدة في نوفمبر 2009 ويناير 2011؛ ما تسبب في وفاة العديد من الأشخاص وألحقت أضرارًا جسيمة بالبنية التحتية، ومن ثمّ أثرت هذه الفيضانات بشكل كبير على ميناء جدة الإسلامي؛ حيث تسببت في تعطيل العمليات وتأخير السفن التي كانت تنتظر التفريغ، كما أدت هذه الفيضانات إلى تضرر الطرق المؤدية إلى الميناء؛ ما عرقل حركة النقل البري أيضًا.[20]

(19) https://www.alarabiya.net/articles, Dust storm in Saudi Arabia, 32009/.

(21) https://ar.wikipedia.org/wiki/ Jeddah floods, 2011.

المطلب الثالث: التحديات الأمنية الحديثة والتطورات التقنية

أولًا: الذكاء الاصطناعي:

تعد تهديدات الذكاء الاصطناعي (Artificial Intelligence) على حركة الملاحة البحريّة في الخليج العربيّ موضوعًا مهمًا يستحق التحليل الدقيق، خاصة في ظل التقدم السريع في التكنولوجيا وتأثيراتها على الأمن البحريّ، ويمكن أن تتمثل التهديدات في التالي:[21]

1. القرصنة المدعومة بالذكاء الاصطناعي (AI–Assisted Piracy): يمكن للذكاء الاصطناعي أن يساعد القراصنة في تحديد الأهداف البحريّة بشكل أكثر دقة وسرعة، باستخدام تقنيات التعرف على الأنماط وتحليل البيانات الكبيرة لتحديد مسارات السفن وشحناتها القيمة مثال: استخدام الطائرات بدون طيار (Drones) المجهزة ببرمجيات الذكاء الاصطناعي لمسح السفن في البحر وتحديد الأهداف المحتملة لهجمات القرصنة.
2. التشويش الإلكتروني (Electronic Jamming): يمكن أن يستخدم الذكاء الاصطناعي لإنشاء تقنيات تشويش إلكتروني معقدة تؤثر على أنظمة الاتصالات والملاحة للسفن؛ ما يجعلها غير قادرة على التواصل أو تحديد مواقعها بدقة مثال: تطوير برمجيات تعتمد على الذكاء الاصطناعي لإنشاء إشارات تشويش؛ ما يؤدي إلى تشويش أو تعطيل أنظمة الملاحة للسفن التجارية.
3. التهديدات الذاتية (Autonomous Threats): الأنظمة الذاتية المدعومة بالذكاء الاصطناعي، مثل الغواصات والطائرات بدون طيار، يمكن أن تستخدم بشكل ضار لتعطيل حركة الملاحة البحريّة من خلال تنفيذ هجمات غير تقليدية أو جمع معلومات استخباراتية مثال: استخدام غواصات ذاتية القيادة مدعومة بالذكاء الاصطناعي لمراقبة حركة السفن التجارية وتحديد الأوقات الأنسب للهجمات أو للاعتراض.

ثانيًا: التهديدات السيبرانية:

الأمن السيبراني والهجمات الإلكترونية على السفن أصبحت من القضايا الملحة في مجال الأمن البحريّ، خاصة في مناطق حيوية كالخليج العربيّ. تستخدم السفن الحديثة أنظمة إدارة تعتمد على التكنولوجيا الرقمية مثل نظم الملاح GPS، ونظام التعريف التلقائي AIS، ونظام الخرائط الإلكترونية ECDIS، وأنظمة الاتصالات والبنية التحتية الحرجة التي تعد عرضة للهجمات الإلكترونية. وقد أدى سباق التسلح الرقمي هذا إلى رفع مستوى الوعي بالتهديدات التي يشكلها التخريب والإرهاب والتجسس الإلكتروني. [22] الهجمات السيبرانية

(21) https://safety4sea.com/steering-with-artificial-intelligence-to-combat-maritime-piracy, 80900 ,2024/

(22) عبد الحفيظ وكمال، آليات حفظ امن البحر الأبيض من الإرهاب البحريّ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 6، ع 1 (2021)، 368.

على السفن والمرافق البحريّة لا تؤدي فقط إلى خسائر اقتصادية كبيرة، بل تعرض أيضًا سلامة وأمن البحارة للخطر. مثال على الهجمات الإلكترونية في الخليج العربيّ الهجوم على أنظمة الملاحة في ميناء الفجيرة: في 2019، فقد تعرض ميناء الفجيرة في الإمارات العربيّة المتحدة لهجوم إلكتروني تسبب في تعطل نظم الملاحة والمراقبة لمدة ساعات؛ ما أثر على حركة السفن ودخولها وخروجها من الميناء. هذا الهجوم أبرز أهمية تأمين البنية التحتية البحريّة ضد التهديدات السيبرانية.[23]

ثالثًا: الطائرات المسيرة والزوارق المسيرة:

لقد شهدت المنطقة عدة حوادث استخدمت فيها هذه الطائرات لتعطيل أو تهديد السفن، وتؤكد الدراسات الأكاديمية والتحليلات الاستراتيجيّة أن التهديدات من الطائرات والزوارق المسيرة تشكل خطرًا حقيقيًا على الملاحة البحريّة في الخليج العربيّ وفقًا لتقرير «مركز الدراسات الاستراتيجيّة والدولية" (CSIS)، فإن زيادة استخدام الطائرات والزوارق المسيرة في الصراعات البحريّة يشير إلى تحول في طبيعة التهديدات البحريّة.

رابعًا: التوترات الأمنيّة في خليج عدن وباب المندب:

يعد باب المندب من أهم الممرات المائية الاستراتيجيّة في العالم؛ حيث يربط بين البحر الأحمر والمحيط الهندي؛ ما يجعله نقطة حيوية للتجارة العالمية، وتشهد منطقة خليج عدن وباب المندب تأثيرات أمنيّة كبيرة تؤثر على حركة الملاحة البحريّة في الخليج العربيّ؛ حيث تعاني هذه المنطقة من تحديات أمنيّة متعددة مثل القرصنة، والصراعات الإقليمية، والتوترات السياسية، والتي تؤدي إلى زيادة المخاطر على السفن التجارية ورفع تكلفة التأمين البحريّ، الملحق رقم (4) يقدم تقييمًا للمخاطر والمهددات التي تواجه حركة الملاحة البحريّة في الخليج العربيّ.

أمثلة للتهديدات الأمنيّة [24]:

1. العام 2011م تم تسجيل 42 حادثة قرصنة في بحر العرب وخليج عدن.
2. العام 2018م انخفاض الحوادث إلى 12 فقط بسبب الدوريات البحريّة المشتركة.
3. العام 2010 – 2015م زيادة في حالات القرصنة البحريّة، خاصة في خليج عدن وبحر العرب.
4. العام 2010 – 2015م هجمات محدودة على السفن والمنشآت البحريّة.
5. العام 2015م – 2024م تصاعد التهديدات خاصة من قبل الجماعات المتطرفة مثل الحوثيين في اليمن الذين استهدفوا ناقلات النفط.

(23) قناة الجزيرة، تعطل ميناء الفجيرة بسبب الهجوم إلكتروني، https://www.google.com/search,2019

(24) https://www.IMO.org/en/OurWork/Security/Pages/Piracy-Reports, 2010 – 2024.

المبحث الثاني: التحليل القانوني للتحديات الأمنيّة

المطلب الأول: التحليل القانوني للتحديات الأمنية التقليدية

أولاً: التحليل القانوني لظاهرة القرصنة البحريّة:

1. التعريف والتمييز: صعوبة تحديد أعمال القرصنة من الناحية القانونية، خاصة في ظل تشابهها مع أعمال إرهابية أو عدائية أخرى في البحر.
2. الاختصاص القضائي: التحديات المرتبطة بتحديد الاختصاص القضائي لمحاكمة القراصنة، خاصة في المياه الدولية أو في الحالات التي يتورط فيها قراصنة من دول متعددة.
3. التنفيذ والتطبيق: ضعف القدرة التنفيذية لبعض الدول على تطبيق القوانين وملاحقة الجناة في حالات القرصنة؛ ما يؤدي إلى الإفلات من العقاب.

ثانيًا: التحليل القانوني لتهديدات الهجرة غير الشرعية / ظاهرة المتسللين (Stowaway):

1. المسؤولية القانونية: يعد الهروب بوسائل غير قانونية من دولة إلى أخرى انتهاكًا للقوانين الوطنية الخاصة بالهجرة والجمارك، ويمكن أن يواجه الهاربون عقوبات تشمل الاحتجاز، أو الغرامات، أو الترحيل.
2. خطر على الحياة: الهروب غالبًا ما يتم في ظروف خطرة؛ ما يعرض حياة الهاربين للخطر، ويمكن أن تتعرض الدول التي تستقبل الهاربين لمسؤوليات قانونية وإنسانية إذا أصيب الهاربون أو ماتوا أثناء المحاولة.
3. التدابير الأمنيّة: يتعين على الدول ووسائل النقل تعزيز تدابيرها الأمنيّة لمنع مثل هذه الحوادث؛ ما يتطلب تحديثات في الأنظمة وتكاليف إضافية.
4. الحماية الدولية: قد يتمتع الهاربون ببعض الحقوق بموجب القانون الدولي، مثل الحق في طلب اللجوء إذا كانوا يفرون من اضطهاد، ومع ذلك يتمثل التحدي في التفريق بين الهاربين الذين يستحقون الحماية بموجب القانون الدولي وأولئك الذين يسعون للهروب لأسباب اقتصادية فقط.
5. المعاملة الإنسانية: تتطلب المعايير الدولية أن تتم معاملة الهاربين بإنسانية، بما في ذلك توفير الطعام والرعاية الصحية أثناء احتجازهم.
6. تبادل المعلومات: الدول بحاجة إلى التعاون في تبادل المعلومات المتعلقة بالهاربين، بما في ذلك التحديد السريع لهويتهم وخلفياتهم.
7. الإعادة القسرية والترحيل والمحاكمة: الاتفاقيات الدولية قد تسهل أو تعيق إعادة الهاربين إلى بلدهم الأصلي، خاصة إذا كان هناك خطر على حياتهم، وبعد القبض على الهاربين قد تبدأ إجراءات قانونية لترحيلهم؛ ما يتطلب احترام حقوقهم القانونية، وقد تختار بعض الدول محاكمة الهاربين على الجرائم المرتبطة بالهروب، مثل الدخول غير القانوني؛ ما يزيد من تعقيد الوضع القانوني.

ثالثًا: التحليل القانوني لظاهرة الإرهاب البحريّ

1. عدم وجود تعريف موحد وتمييزه عن الجرائم الأخرى: رغم وجود اتفاقيات دولية لمكافحة الإرهاب، إلا أنه لا يوجد تعريف محدد ومتفق عليه دوليًا للإرهاب البحريّ؛ ما يخلق صعوبة في تحديد ما يشكل عملًا إرهابيًا في البحر. يجب التفريق بين الإرهاب البحريّ وأشكال أخرى من الجرائم البحريّة مثل القرصنة أو التهريب؛ حيث إن لكل منها إجراءات قانونية مختلفة.
2. الولايات القضائية المتداخلة: الإرهاب البحريّ غالبًا ما يقع في مناطق خارج نطاق الولاية الوطنية (المياه الدولية)؛ ما يثير تساؤلات حول أي دولة لديها الحق في محاكمة المتهمين، خاصة إذا كانت الدول المتضررة متعددة.
3. معاملة المشتبه بهم والاحتجاز: يجب على الدول الالتزام بالقوانين الدولية لحقوق الإنسان عند اعتقال أو محاكمة المشتبه بهم في الإرهاب البحريّ، بما في ذلك حظر التعذيب وضمان محاكمات عادلة، وقد يؤدي احتجاز المشتبه بهم لفترات طويلة دون محاكمة إلى انتهاكات لحقوق الإنسان؛ ما يعقد الإجراءات القانونية ويعرض الدول للمساءلة الدولية.
4. حماية السفن والبنية التحتية البحريّة من التهديدات غير التقليدية: حماية السفن التجارية والبنية التحتية البحريّة (مثل الموانئ وخطوط الأنابيب تحت البحر) تتطلب تدابير أمنيّة مشددة، بما في ذلك التعاون بين القطاعين العام والخاص. ويضيف استخدام الإرهابيين لتكتيكات غير تقليدية مثل الهجمات الانتحارية أو العبوات الناسفة البدائية في البحر طبقة إضافية من التعقيد في التصدي لهذه التهديدات.
5. العقوبات والمساءلة: تطبيق العقوبات الدولية ضد الدول أو الأفراد الذين يدعمون الإرهاب البحريّ يمثل تحديًا قانونيًا، خاصة إذا كانت هناك صعوبة في إثبات تورطهم المباشر.

المطلب الثاني: التحليل القانوني للحوادث والجرائم البحرية

أولًا: التحليل القانوني للحوادث البحريّة في الخليج العربيّ:

1. الاختصاص القضائي والتداخل القانوني للحدود البحريّة المتنازع عليها: يؤدي النزاع على الحدود البحريّة إلى تداخل الاختصاصات القضائية هذا التداخل يمكن أن يعقد التحقيقات في الحوادث البحريّة ويعرقل عملية تحديد المسؤولية.
2. المياه الإقليمية والمياه الدولية: تختلف القوانين المطبقة على الحوادث البحريّة حسب ما إذا كانت الحادثة وقعت في المياه الإقليمية لدولة معينة أو في المياه الدولية. في المياه الإقليمية، تطبق القوانين الوطنية، بينما في المياه الدولية يتم الاعتماد على الاتفاقيات الدولية مثل اتفاقية الأمم المتحدة لقانون البحار (UNCLOS).

3. مسؤولية السفن والأطراف المعنية: في حالة وقوع حادث بحريّ، مثل تصادم السفن أو تسرب النفط، يصبح تحديد الطرف المسؤول أمرًا معقدًا، خاصة إذا كانت السفن مسجلة في دول مختلفة وتعمل تحت أعلام مختلفة.
4. التعويضات وإصلاح الأضرار: تحديد المسؤولية عن الأضرار، سواء البيئية أم الاقتصادية، قد يتطلب إجراءات قانونية طويلة ومعقدة، وتشمل هذه المسؤولية تعويض الدول المتضررة أو الشركات المتضررة، بالإضافة إلى إصلاح الأضرار البيئية.
5. الحوادث الناجمة عن التهديدات الأمنيّة: الخليج العربيّ يشهد توترات سياسية وأمنيّة؛ ما يزيد من خطر الحوادث البحريّة الناجمة عن الهجمات أو الأعمال التخريبية هذه الحوادث تؤدي إلى تحديات قانونية إضافية تتعلق بالتحقيق وتحديد المسؤولية في ظل الظروف الأمنيّة المضطربة.
6. حماية الممرات البحريّة: التهديدات الأمنيّة تتطلب من الدول تعزيز التدابير الأمنيّة لحماية الممرات البحريّة (مضيق هرمز)، وهو ما قد يؤثر على حرية الملاحة ويسبب تعقيدات قانونية تتعلق بحق المرور العابر.
7. تعطل حركة الملاحة البحريّة: أي حادث كبير في الخليج العربيّ يمكن أن يؤدي إلى تعطيل كبير لحركة الملاحة؛ ما يؤثر على التجارة العالمية والتحدي القانوني هنا يكمن في التعامل مع الخسائر الاقتصادية وتعويض الأطراف المتضررة.
8. التحقيقات والاتفاقيات الدولية: في حالة وقوع حوادث بحريّة كبيرة، قد يتم إجراء تحقيقات دولية لتحديد الأسباب والمسؤوليات والتعاون بين الدول في هذا الصدد قد يواجه تحديات بسبب اختلاف الأنظمة القانونية والمعايير الفنية. تعتمد معالجة الحوادث البحريّة في الخليج العربيّ على تطبيق الاتفاقيات الدولية مثل اتفاقية الأمم المتحدة لقانون البحار (UNCLOS) واتفاقيات أخرى متعلقة بالسلامة البحريّة والتلوث، ولكن قد تواجه هذه الاتفاقيات تحديات في التنفيذ بسبب التوترات السياسية أو عدم الامتثال الكامل من قبل بعض الدول.
9. تحقيقات الحوادث البحريّة: تتطلب استخدام تقنيات متقدمة لجمع الأدلة وتحديد الأسباب؛ ما قد يفرض تحديات تقنية وقانونية خاصة في تحديد المسؤوليات.

ثانيًا: التحليل القانوني لجرائم التهريب Smuggling:

تنوع أنشطة التهريب: يشمل التهريب البحريّ مجموعة واسعة من الأنشطة غير القانونية، مثل تهريب المخدرات، الأسلحة، البضائع المقلدة، والأشخاص. تحدد القوانين الوطنية والدولية هذه الأنشطة بشكل مختلف؛ ما يصعب من توحيد الجهود القانونية لمكافحته.

1. التفريق بين الجرائم: قد يصعب التفريق بين التهريب البحريّ وجرائم بحريّة أخرى مثل القرصنة أو الإرهاب البحريّ؛ حيث قد تتداخل هذه الأنشطة أو تستخدم وسائل متشابهة.
2. الاختصاص القضائي: (المياه الدولية مقابل المياه الإقليمية) يحدث التهريب البحريّ غالبًا في المياه الدولية، حيث لا توجد ولاية قضائية واضحة لدولة واحدة؛ ما يعقد عملية الاعتقال والمقاضاة.
3. تطبيق القوانين والتشريعات الوطنية: عندما يتم القبض على المهربين في المياه الإقليمية، تطبق الدولة المعنية قوانينها الوطنية، ولكن قد تواجه صعوبة في تقديم الأدلة أو تطبيق العقوبات في حالات التهريب التي تشمل أكثر من دولة.
4. الاختلافات القانونية: تواجه الدول تحديات في التعاون بسبب اختلاف القوانين والإجراءات القضائية؛ ما قد يعرقل الجهود المشتركة لضبط المهربين وملاحقتهم قضائيًا.
5. تطور أساليب التهريب: يعتمد المهربون على تقنيات وأساليب متطورة لتجنب الكشف، مثل استخدام السفن الصغيرة التي يصعب رصدها، الغواصات الصغيرة، أو حتى الطائرات بدون طيار. هذا يتطلب من السلطات البحريّة تطوير تقنيات مراقبة واستخبارات متقدمة.
6. التهديدات المرتبطة بالتهريب: يمكن أن يسهم التهريب البحريّ في تمويل أنشطة إجرامية أخرى، مثل الإرهاب أو الاتجار بالبشر؛ ما يزيد من التحديات الأمنيّة للدول المعنية.
7. الاتجار بالبشر: يشكل تهريب الأشخاص (بما فيهم المجرمون الفارون من القانون) عبر البحر انتهاكًا خطيرًا لحقوق الإنسان، ويضع تحديات قانونية كبيرة، مثل تحديد الضحايا وتوفير الحماية لهم.
8. العقوبات الدولية: تطبيق العقوبات ضد الدول أو الأفراد المتورطين في التهريب البحريّ يمثل تحديًا، خاصة إذا كانت هناك صعوبات في إثبات المسؤولية المباشرة أو في الحصول على الدعم الدولي لتطبيق العقوبات.

ثالثًا: التحليل القانوني للأضرار البيئية:

1. تعدد الأطراف المسؤولة: يمكن أن يكون التلوث البحريّ ناتجًا عن عدة مصادر مثل السفن، منصات النفط، المصانع الساحلية، أو حتى الدول نفسها. هذا التعدد يعقد عملية تحديد المسؤول عن التلوث، سواء كان شركة أم دولة؛ ما يصعب تحديد الطرف الذي يجب أن يتحمل تكاليف التنظيف والتعويضات.
2. إثبات المسؤولية: في كثير من الحالات، يكون من الصعب إثبات العلاقة المباشرة بين مصدر التلوث والأضرار الناجمة عنه، خاصة في الحالات التي يتداخل فيها التلوث من مصادر متعددة.

3. اختلاف القوانين والتشريعات الوطنية: تختلف القوانين البيئية من دولة إلى أخرى؛ ما يؤدي إلى تفاوت في كيفية معالجة التلوث البحريّ وتطبيق القوانين. بعض الدول قد تكون لديها قوانين صارمة، بينما قد تكون دول أخرى أقل التزامًا بالمعايير البيئية؛ ما يخلق تحديًا في تنفيذ الاتفاقيات الدولية بشكل متساوٍ.

4. التنفيذ والامتثال: حتى مع وجود اتفاقيات دولية مثل «اتفاقية ماربول» (MARPOL) التي تهدف إلى منع التلوث البحريّ من السفن، فإن تنفيذ هذه الاتفاقيات يعتمد على التزام الدول وفعاليتها في تطبيقها، وقد تواجه بعض الدول تحديات في تنفيذ هذه الاتفاقيات بسبب نقص الموارد أو البنية التحتية.

5. التلوث العابر للحدود: التلوث البحريّ غالبًا ما يكون عابرًا للحدود؛ حيث ينتقل التلوث من منطقة إلى أخرى بفعل التيارات البحريّة. هذا يثير تساؤلات حول المسؤولية القانونية للدول التي يتسبب تلوثها في أضرار لدول أخرى.

6. تكاليف التنظيف والتعويضات: تكاليف تنظيف التلوث البحريّ وإصلاح الأضرار البيئية يمكن أن تكون باهظة للغاية، وهناك تحديات قانونية في توزيع هذه التكاليف على الأطراف المسؤولة، وقد يؤدي ذلك إلى نزاعات قانونية طويلة ومعقدة.

7. التأثير على الصناعات البحريّة: التلوث البحريّ يمكن أن يؤثر سلبًا على صناعات مثل الصيد، والسياحة، والشحن البحريّ. الشركات المتضررة قد تطالب بتعويضات؛ ما يضيف بعدًا آخر للتحديات القانونية.

8. حماية المجتمعات الساحلية والصحة العامة: قد يؤدي التلوث البحريّ إلى تدمير مصادر الرزق للمجتمعات الساحلية التي تعتمد على الصيد أو السياحة، فهذه المجتمعات قد ترفع قضايا للمطالبة بحقوقها؛ ما يخلق تحديات قانونية تتعلق بحماية حقوق الإنسان، فالتلوث البحريّ قد يؤدي إلى تلوث موارد المياه والأسماك؛ ما يؤثر على صحة الإنسان والقضايا القانونية قد تتعلق بتعويضات الصحة العامة وإجراءات الوقاية.

9. جمع الأدلة: التلوث البحريّ غالبًا ما يتطلب تقنيات متقدمة لجمع الأدلة وتحليلها لتحديد مصدر التلوث، وهذا يشمل استخدام الأقمار الصناعية، والرادارات، والتحليل الكيميائي، ويكمن التحدي هنا في تأمين الأدلة الموثوقة التي يمكن استخدامها في المحاكم.

10. نقص الوعي القانوني: قد يكون هناك نقص في الوعي بين الأطراف المعنية، مثل مالكي السفن أو الشركات الصناعية، حول القوانين المتعلقة بالتلوث البحريّ، ويؤدي هذا إلى تحديات في الامتثال ويزيد من الحاجة إلى تدريب وتوعية أفضل.

11. تعزيز القدرات القانونية: تحتاج الدول إلى تطوير قدراتها القانونية والفنية للتعامل مع قضايا التلوث البحريّ، بما في ذلك تدريب القضاة والمحامين والمسؤولين الحكوميين على القوانين والاتفاقيات البيئية.

12. الاستجابة للطوارئ / خطط الطوارئ: حوادث التلوث البحريّ الكبيرة، مثل التسربات النفطية، تتطلب استجابة سريعة ومنسقة. التحدي القانوني هنا يكمن في التنسيق بين الجهات المعنية وتحديد المسؤوليات القانونية في حالات الطوارئ. قد تواجه الدول تحديات في وضع وتنفيذ خطط طوارئ فعالة تستجيب لحوادث التلوث البحريّ الكبيرة، وتتطلب هذه الخطط التعاون بين القطاعين العام والخاص. وتعد حماية البيئة البحريّة في الخليج العربيّ من الأمور الحيوية التي ترتبط بشكل مباشر بقضايا الأمن البحريّ وحركة الملاحة البحريّة، وتشهد المنطقة كثافة مرورية عالية للسفن التجارية وناقلات النفط.

المطلب الثالث: التحليل القانوني للتحديات التقنية الحديثة والصيد الجائر

أولاً: التحليل القانوني لتهديدات الأمن السيبراني / الذكاء الاصطناعي :

1. الهجمات السيبرانية على البنية التحتية الحساسة: مع زيادة استخدام الذكاء الاصطناعي في البنية التحتية الحيوية مثل الكهرباء، والمياه، والنقل، يتزايد خطر الهجمات السيبرانية؛ ما يتطلب لحماية هذه الأنظمة قوانين وسياسات أمنيّة متقدمة.
2. القرصنة السيبرانية: الهجمات السيبرانية قد تستهدف سرقة الملكية الفكرية أو بيانات حساسة؛ ما يخلق تحديات قانونية حول كيفية حماية حقوق الملكية الفكرية في العالم الرقمي.
3. تعقب الجرائم السيبرانية: الطبيعة العابرة للحدود للجرائم السيبرانية تجعل من الصعب تعقب المجرمين وتقديمهم للعدالة. يتطلب ذلك تطوير آليات قانونية دولية فعالة للتعاون في إنفاذ القانون.
4. المساءلة في الأمن السيبراني: في حالة وقوع هجمات سيبرانية على أنظمة ذكاء اصطناعي، تصبح المساءلة القانونية معقدة. تحديد الجهة المسؤولة عن الأضرار الناجمة عن الاختراقات يتطلب تشريعات واضحة.
5. السباق التكنولوجي: الدول تسعى إلى تطوير تقنيات الذكاء الاصطناعي للدفاع الوطني، ولكن ذلك يثير تحديات قانونية تتعلق بتنظيم استخدام الذكاء الاصطناعي في المجال العسكري وضمان عدم وقوع هذه التقنيات في أيدي الجماعات الإرهابية.
6. تحديث التشريعات: التطورات السريعة في مجالي الأمن السيبراني والذكاء الاصطناعي تتطلب تحديثًا مستمرًا للتشريعات لتنظيم استخدامات الذكاء الاصطناعي أو حماية البنية التحتية السيبرانية.
7. التهديدات السيبرانية عابرة للحدود: ما يتطلب تعاونًا دوليًا وإطارًا قانونيًا موحدًا. ومع ذلك، فإن الاختلافات في القوانين والسياسات بين الدول تشكل تحديًا كبيرًا.

8. التصميم الأخلاقي للذكاء الاصطناعي: تطوير أنظمة ذكاء اصطناعي تتخذ قرارات بناءً على خوارزميات قد يؤدي إلى نتائج غير عادلة أو تمييزية. التحدي القانوني هنا هو كيفية ضمان أن تكون هذه الأنظمة أخلاقية ومنصفة. وضع قوانين تنظم الأخلاقيات في استخدام الذكاء الاصطناعي يتطلب توازنًا بين الابتكار وحماية حقوق الإنسان. ذلك يشمل معالجة قضايا مثل التحيز الخوارزمي واستخدام الذكاء الاصطناعي في المجالات الحساسة كالرعاية الصحية والعدالة الجنائية.
9. تقنيات الهجوم المتقدمة: مع تقدم الذكاء الاصطناعي، تتطور أيضًا تقنيات الهجوم السيبراني؛ ما يزيد من تعقيد التحديات القانونية المتعلقة بأمن الشبكات وحماية البيانات.
10. انتهاك الخصوصية: مع تزايد استخدام الذكاء الاصطناعي في جمع وتحليل البيانات الشخصية، تنشأ تحديات قانونية كبيرة تتعلق بحماية خصوصية الأفراد ووضع قوانين وتشريعات حماية البيانات.
11. إدارة البيانات الكبيرة (Big Data): الذكاء الاصطناعي يعتمد بشكل كبير على تحليل كميات هائلة من البيانات. جمع هذه البيانات ومعالجتها قد يؤدي إلى مشكلات قانونية تتعلق بحقوق الملكية الفكرية، الخصوصية، والأخلاقيات.
12. المساءلة والمسؤولية القانونية عن الأفعال الخاطئة للذكاء الاصطناعي: في حال ارتكب نظام ذكاء اصطناعي خطأً أدى إلى أضرار مالية أو جسدية، يكون من الصعب تحديد المسؤولية القانونية ومن يجب أن يتحمل المسؤولية؟ المطور؟ أم المشغل؟ أم النظام نفسه؟

ثانيًا: التحليل القانوني لتهديدات الطائرات المسيرة (الدرونز) / الزوارق المسيرة:

1. نقص التشريعات الواضحة: الطائرات والزوارق المسيرة لا تزال تقنية حديثة، وبالتالي قد تكون القوانين الحالية غير كافية لتنظيم استخدامها. هناك حاجة لتحديث التشريعات الوطنية والدولية لتشمل التعريفات الواضحة والضوابط المتعلقة بهذه التقنيات.
2. التصنيف القانوني: تحديد ما إذا كانت الطائرات والزوارق المسيرة تعد سفنًا أو طائرات وفقًا للقانون الدولي يؤثر على القوانين التي تنطبق عليها؛ ما يخلق تحديًا في تنظيمها ضمن الأطر القانونية الحالية.
3. تهديد السلامة البحريّة: الطائرات والزوارق المسيرة يمكن أن تشكل خطرًا على السفن والبنية التحتية البحريّة، خاصة إذا استخدمت بشكل غير قانوني أو عدائي. التحدي القانوني يكمن في كيفية تنظيم استخدام هذه الأجهزة لضمان عدم تعريض سلامة الملاحة البحريّة للخطر.

4. استخدامها كأدوات هجوم: يمكن استخدام الطائرات والزوارق المسيرة في هجمات إرهابية أو قرصنة بحريّة. هذا يثير قضايا قانونية حول كيفية التصدي لهذه التهديدات ومنعها، بما في ذلك القوانين التي تسمح بإسقاط أو تعطيل الأجهزة المسيرة في حالات الطوارئ.
5. تداخل الاختصاص القضائي: إذا تم استخدام طائرة أو زورق مسير في هجوم أو نشاط غير قانوني في مياه دولية أو في مناطق ذات اختصاصات متداخلة، فإن ذلك يخلق تحديات قانونية معقدة تتعلق بمن يملك الحق في التدخل أو ملاحقة المسؤولين.
6. المراقبة غير المشروعة: الطائرات والزوارق المسيرة يمكن استخدامها لجمع معلومات استخباراتية أو للتجسس على السفن والمرافق البحريّة؛ ما يثير قضايا قانونية تتعلق بانتهاك الخصوصية والحقوق السيادية للدول.
7. غياب اتفاقيات دولية محددة: حتى الآن، لا توجد اتفاقيات دولية شاملة تنظم استخدام الطائرات والزوارق المسيرة في المياه الدولية أو تحدد كيفية التعامل مع التهديدات التي تشكلها على الملاحة البحريّة. هذا الفراغ القانوني يمثل تحديًا كبيرًا للدول التي تسعى لضمان أمن وسلامة ممراتها البحريّة.
8. تحديات تنفيذ القانون: إن فرض القوانين على الطائرات والزوارق المسيرة في البحر يمكن أن يكون معقدًا بسبب صغر حجمها، سرعتها العالية، وصعوبة اكتشافها. هناك حاجة لتطوير تقنيات رصد ومراقبة فعالة يمكن استخدامها لتطبيق القوانين والتشريعات الوطنية.
9. الاستجابة السريعة: في حالة استخدام الطائرات والزوارق المسيرة لأغراض عدائية ضد السفن والموانئ والمرافق البحريّة، يتطلب الأمر استجابة قانونية وعسكرية سريعة. ومع ذلك، فإن القدرة على تحديد مصدر هذه الأجهزة ومن يقف وراءها بشكل قانوني قد يكون معقدًا.
10. التحكم عن بعد والذكاء الاصطناعي: استخدام الذكاء الاصطناعي والتحكم عن بعد في الطائرات والزوارق المسيرة يزيد من التعقيدات القانونية، خاصة فيما يتعلق بالمسؤولية عن الأضرار التي قد تنجم عن أخطاء أو خلل تقني.

ثالثًا: التحليل القانوني لمهددات الصيد الجائر:

1. تطبيق القانون: هناك قوانين وتشريعات تحظر الصيد الجائر وتحدد الحصص المسموح بها وأوقات الصيد المسموح بها، لكن التحدي يكمن في تطبيق هذه القوانين بفعالية؛ حيث قد تكون هناك صعوبة في المراقبة المستمرة للأنشطة البحريّة في الخليج العربيّ بسبب مساحته الواسعة وتعدد الدول المطلة عليه.
2. التعاون الإقليمي: يتطلب مكافحة الصيد الجائر تعاونًا بين دول الخليج العربيّ وقد يؤدي ضعف التعاون بين الدول في تطبيق القوانين والإجراءات المشتركة إلى فشل الجهود في حماية الموارد البحريّة.

3. تكنولوجيا المراقبة والمتابعة: تعتمد مراقبة الصيد الجائر على استخدام تكنولوجيا متطورة مثل أنظمة تتبع السفن والأقمار الصناعية، لكن بعض الدول قد تواجه تحديات التكاليف والتقنية في تبني مثل هذه التكنولوجيا أو في تطوير القدرات البشرية اللازمة لإدارتها.
4. العقوبات: العقوبات على الصيد الجائر قد تكون غير كافية لردع المخالفين. في بعض الحالات، العقوبات المالية أو السجن قد لا تكون رادعة بما فيه الكفاية إذا ما قورنت بالأرباح الكبيرة التي يمكن أن يجنيها الصيادون من ممارسات الصيد الجائر.
5. التحديات البيئية: يؤثر الصيد الجائر على التوازن البيئي في الخليج العربيّ، ويؤدي إلى استنزاف الأنواع البحريّة وزعزعة النظم البيئية. يتطلب مواجهة هذا التحدي وجود قوانين بيئية صارمة ومطبقة بفعالية، وكذلك تطبيق برامج توعية للحفاظ على البيئة البحريّة.

الفصل الثاني
انعكاسات التحديات الأمنيّة وعلاقتها بحركة الملاحة البحريّة في الخليج العربيّ

تمهيد:

تُعد منطقة الخليج العربيّ إحدى أهم المناطق الاستراتيجيّة في العالم بسبب موقعها الحيوي واحتضانها لأكبر مصادر الطاقة العالمية، ومع ذلك تواجه حركة الملاحة البحريّة في الخليج تحديات أمنيّة متزايدة تهدد استقرارها، ومن أبرز هذه التحديات تهديدات القرصنة، والعمليات الإرهابية، والتوترات السياسية بين دول المنطقة. كما تُعد النزاعات الإقليمية، مثل تلك المتعلقة بالمضائق البحريّة الحيوية كمضيق هرمز، من أبرز العوامل المؤثرة على حركة السفن التجارية والإمدادات النفطية. هذه التحديات الأمنيّة لا تؤثر فقط على استقرار الملاحة البحريّة، بل تحمل انعكاسات سلبية على الاقتصاد العالمي والقدرة على تأمين خطوط الإمداد البحريّة. تم تقسيم هذا الفصل كالتالي:

المبحث الأول: حركة الملاحة البحريّة وتأثيرات الأمن البحريّ
المبحث الثاني: تأثيرات التحديات الأمنيّة المختلفة على حركة الملاحة البحريّة في الخليج العربيّ

المبحث الأول
حركة الملاحة البحريّة وتأثيرات الأمن البحريّ

المطلب الأول: حركة الملاحة في الخليج العربيّ

1. حركة الملاحة البحريّة في الخليج العربيّ تؤدي دورًا حيويًا في الاقتصاد العالمي؛ نظرًا لكون المنطقة أحد أكبر مراكز إنتاج وتصدير النفط والغاز الطبيعي، كما يشهد الخليج

العربيّ مرور نحو 30% من شحنات النفط العالمية ويمثل بذلك أحد أهم الممرات المائية الاستراتيجيّة في العالم تتركز حركة الملاحة في مضيق هرمز، الذي يعد ممرًا حيويًا يربط الخليج العربيّ بالمحيط الهندي، ويشهد عبور ما يقرب من 20 مليون برميل من النفط يوميًا. [25]

2. هناك تحديات وتهديدات تعترض حركة الملاحة البحريّة في الخليج العربيّ تشمل التهديدات الأمنيّة مثل القرصنة والإرهاب البحريّ، والتلوث البحريّ الناتج عن التسربات النفطية وحوادث السفن، كما تشكل التوترات السياسية وتوتر العلاقات تهديدًا مستمرًا لحركة الملاحة؛ حيث شهدت المنطقة حوادث استهداف السفن وتهديدات بإغلاق مضيق هرمز في فترات التوتر الشديد، الملحق رقم (1) يوضح خرائط للخليج العربيّ وباب المندب.
3. تشير الدراسات إلى أن الاستثمارات الكبيرة في البنية التحتية للموانئ، وتطوير الأنظمة الأمنيّة الحديثة، وتعزيز التعاون الدولي أسهمت في تعزيز أمن وسلامة حركة الملاحة في الخليج العربيّ. ووفقًا لتقرير «مؤسسة الدراسات البحريّة الدولية" (International Maritime Studies Institute) في 2020، فإن تحديث الموانئ وتطبيق التقنيات المتقدمة في رصد وتتبع السفن ساعد في تحسين كفاءة العمليات البحريّة وتقليل وقت الانتظار في الموانئ الخليجية.

المطلب الثاني: أهمية وتأثير الأمن البحريّ في الخليج العربيّ:

يعد الأمن البحريّ في الخليج العربيّ ذا أهمية بالغة نظرًا للموقع الجغرافي الاستراتيجي الذي تحتله هذه المنطقة، بالإضافة إلى احتضانها لمصادر طاقة حيوية للعالم، يؤثر الأمن البحريّ في الخليج العربيّ على جوانب متعددة تشمل الاقتصادية والأمنيّة:[26]

1. حماية خطوط التجارة الدولية: يمثل الخليج العربيّ ممرًا حيويًا لخطوط الملاحة البحريّة التي تنقل النفط والغاز الطبيعي إلى مختلف أنحاء العالم، وقد يؤدي أي تهديد لأمن هذه الخطوط إلى اضطرابات في إمدادات الطاقة العالمية؛ ما ينعكس سلبًا على الاقتصاد الدولي.
2. مكافحة الأنشطة غير القانونية: يؤدي الأمن البحريّ دورًا مهمًا في مكافحة القرصنة والتهريب والاتجار بالبشر والأسلحة، ولا تهدد هذه الأنشطة غير القانونية فقط الأمن الإقليمي ولكنها تسهم أيضًا في تمويل الجماعات الإرهابية والمليشيات غير الشرعية.
3. ضمان استقرار الأسواق النفطية: الخليج العربيّ يحتوي على بعض أكبر احتياطيات النفط في العالم، وأي تهديد لأمن الموانئ والمنشآت النفطية قد يؤدي إلى ارتفاع أسعار النفط

(25) Khalid, I, Maritime Security in the Gulf Region. Naval War College Review, (2007) 65(4), 7290-. link: Naval War College Review - Digital Common.

(26) UNCLOS, United Nations Convention on the Law of the Sea, 1982,100107-. UNCLOS Text on UN.org,UN Office of Legal Affairs.

على المستوى العالمي؛ ما يؤثر على الاستقرار الاقتصادي للدول المنتجة والمستهلكة على حد سواء.

4. الحفاظ على البيئة البحريّة: تتعرض البيئة البحريّة في الخليج العربيّ لتهديدات من الأنشطة غير القانونية مثل الصيد الجائر والتلوث البحريّ، ويسهم الأمن البحريّ في حماية النظم البيئية البحريّة والحفاظ على التنوع البيولوجي.

المبحث الثاني: تأثيرات التحديات الأمنيّة على حركة الملاحة في الخليج العربيّ

المطلب الأول: التأثيرات الأمنية المباشرة على حركة الملاحة البحرية

أولاً: تأثيرات القرصنة البحريّة:

1. زيادة تكاليف التأمين والحراسة.
2. تعطيل التجارة أو تقليل النقل البحريّ.
3. تدخلات عسكرية لحماية حركة الملاحة (القيود التي تفرض بسبب الوجود العسكري).
4. خسائر الاقتصادات المحلية الناتجة عن تعطل حركة الملاحة.
5. تأثر الصناعات المحلية (الصيد والسياحة) قد تكون أكثر عرضة لهجمات القراصنة.

ثانيًا: تأثيرات الهجرة غير الشرعية:

1. زيادة المراقبة والإجراءات الأمنيّة وهذا يؤدي إلى تفتيش السفن تفتيشًا متكررًا وتأخير مرورها؛ ما يؤثر سلبًا على حركة الملاحة والتجارة.
2. تهديدات السلامة البحريّة؛ إذ إن الهاربين عادة ما يستخدمون قوارب غير آمنة ومكتظة؛ ما يزيد من احتمالية وقوع حوادث بحريّة، وقد يؤدي وقوع مثل هذه الحوادث في ممرات بحريّة رئيسة إلى تعطيل حركة الملاحة وفرض قيود مؤقتة على المرور.
3. يمكن أن يستغل بعض الأفراد أو الجماعات غير الشرعية هذا النوع من الهجرة لتهريب الأسلحة أو القيام بأعمال إرهابية في الخليج العربيّ، وتزيد هذه التهديدات في المنطقة وتجعل الدول أكثر حذرًا في السماح للسفن بالمرور؛ ما يؤثر على التدفق الحر لحركة الملاحة.
4. تعطيل حركة الملاحة بسبب الهجرة غير الشرعية يمكن أن يؤدي إلى تأخير وصول البضائع وزيادة تكاليف النقل البحريّ؛ ما يؤثر سلبًا على التجارة الإقليمية والدولية.

ثالثًا: تأثيرات الإرهاب البحريّ:

1. بسبب التهديدات الإرهابية، تضطر الدول والشركات إلى تعزيز الإجراءات الأمنيّة لحماية السفن والبنية التحتية البحريّة، ويشمل هذا استخدام السفن الحربية للمرافقة، ونشر

القوات العسكرية في مناطق استراتيجيّة، وزيادة المراقبة والرصد، وقد تؤدي هذه الإجراءات إلى تأخير حركة السفن وزيادة تكاليف النقل.

2. الهجمات الإرهابية قد تستهدف السفن أو المنشآت البحريّة مثل الموانئ ومنصات النفط. إذا ما تعرضت هذه البنية التحتية لهجمات، يمكن أن يتم إغلاق أجزاء من الخليج أو فرض قيود على حركة السفن؛ ما يؤدي إلى تعطيل طرق الملاحة وتوقف الأنشطة التجارية.
3. زيادة التوترات الجيوسياسية: يمكن أن تؤدي الهجمات الإرهابية في الخليج العربيّ إلى تصاعد التوترات بين الدول الإقليمية والدولية، وقد يؤدي هذا التصعيد إلى زيادة الوجود العسكري الأجنبي في المنطقة؛ ما يزيد من المخاطر المحتملة على حركة الملاحة.

رابعًا: تأثيرات التهريب:

1. التهريب، سواء كان تهريب الأسلحة، أم المخدرات، أم البضائع، أم حتى البشر، يؤدي إلى زيادة الحاجة إلى تعزيز الإجراءات الأمنيّة والمراقبة في الخليج العربيّ.
2. الدول المطلة على الخليج العربيّ وكذلك القوات البحريّة الدولية ستقوم بزيادة الدوريات، والتفتيش، والمراقبة باستخدام تقنيات حديثة، وقد تؤدي هذه الإجراءات إلى تأخير السفن وتباطؤ حركة الملاحة.

خامسًا: تأثيرات الحوادث البحريّة :

1. إغلاق المسارات البحريّة: في حالة وقوع حادث كبير، قد يتم إغلاق أجزاء من المسارات البحريّة لتسهيل عمليات الإنقاذ أو لاحتواء التلوث البيئي؛ ما يؤدي إلى تأخير حركة السفن وانتظارها لفترات طويلة.
2. تحويل المسارات: قد تضطر السفن إلى تغيير مساراتها لتجنب المناطق المتأثرة بالحوادث؛ ما يزيد من وقت الرحلات والتكاليف التشغيلية.

سادسًا: تأثيرات التوترات الأمنيّة والسياسية:

1. تأخير الشحنات وتقليل حركة السفن.
2. الانعكاس السلبي على اقتصاديات الدول المطلة على الخليج العربيّ والتي تعتمد اعتمادًا كبيرًا على صادرات النفط والغاز والتجارة الدولية عبر هذا الممر البحريّ.

المطلب الثاني: التأثيرات التقنية والبيئية على حركة الملاحة البحرية

أولًا: تأثيرات المعوقات التقنية والإدارية :

1. المشاكل التقنية: قد تؤدي الأعطال في الأنظمة الإلكترونية والميكانيكية للسفن أو في البنية التحتية للموانئ (مثل الرافعات أو أنظمة التحكم في الحركة) إلى تأخير عمليات الشحن والتفريغ؛ ما يؤخر حركة السفن.

2. الإجراءات الإدارية المعقدة: التعقيدات في الإجراءات الجمركية، وإجراءات التفتيش والتوثيق، قد تؤدي إلى تأخير غير مبرر في تصاريح المرور أو إتمام عمليات الشحن؛ ما يعيق حركة الملاحة ويسبب تراكم السفن في الموانئ.

ثانيًا: تأثيرات الذكاء الاصطناعي والأمن السيبراني:

1. التشويش على الأنظمة الإلكترونية لتشغيل الموانئ والسفن.
2. التشويش على منظومات إدارة العمليات البحريّة المختلفة؛ ما يؤدي لتعطيل حركة الملاحة البحريّة.

ثالثًا: تأثيرات الطائرات المسيرة والزوارق المسيرة:

1. استخدامها غير القانوني في مراقبة ومتابعة السفن.
2. إمكانية تجهيز الطائرات والزوارق المسيّرة بأسلحة أو متفجرات تُستخدم لمهاجمة السفن المستهدفة.
3. استهداف المنشآت البحريّة الحساسة مثل منصات النفط، الموانئ، أو السفن الحربية، سواء عبر الهجمات التفجيرية أم جمع المعلومات الاستخباراتية.
4. استخدامها في هجمات انتحارية تستهدف السفن أو البنية التحتية الحيوية في الموانئ.
5. تأثير نفسي وإعلامي قوي؛ إذ يصعب توقع هذه الهجمات أو التصدي لها في بعض الأحيان.
6. نقل المخدرات والأسلحة بين الشواطئ والسفن في عرض البحر؛ ما يتيح للمهربين تجنب دوريات خفر السواحل أو السلطات البحريّة.
7. القدرة على العمل ليلًا وفي ظروف الطقس السيئة تجعل المسيّرات وسيلة فعالة في تفادي مراقبة الرادارات والأنظمة التقليدية، كما يمكن أن تُستخدم للطيران على ارتفاعات منخفضة لتجنب الكشف.

رابعًا: تأثيرات التغيرات المناخية:

1. انخفاض الرؤية: تؤدي العواصف الرملية والغبارية المتكررة إلى انخفاض الرؤية، مما يزيد من مخاطر الاصطدام والحوادث البحريّة، وتتطلب السفن زيادة الحذر وتقليل السرعة؛ ما يؤدي إلى تأخير الشحنات وارتفاع تكاليف التأمين.
2. ارتفاع تكاليف الصيانة: تؤدي الظروف الجوية القاسية إلى زيادة تآكل وتلف البنية التحتية البحريّة والسفن؛ ما يزيد من تكاليف الصيانة والإصلاح، وتحتاج الموانئ إلى تعزيز هياكلها لمقاومة العواصف وارتفاع مستوى سطح البحر.

3. اضطراب سلاسل التوريد: تؤدي الظواهر الجوية القاسية إلى تعطيل سلاسل التوريد العالمية؛ حيث تعتمد العديد من الدول على الواردات والصادرات عبر موانئ الخليج العربيّ، وتؤدي التأخيرات والتعطيلات إلى نقص في الإمدادات وزيادة تكاليف النقل.

خامسًا: تأثيرات التلوث البحريّ :

1. إغلاق الممرات المائية: في حالات التلوث البحريّ الشديد، مثل التسربات النفطية الكبيرة، قد يتم إغلاق أجزاء من الممرات المائية لتسهيل عمليات التنظيف وحماية البيئة البحريّة، ويؤدي هذا إلى تعطيل حركة السفن وتأخير عمليات الشحن والتفريغ.
2. تحويل المسارات: السفن قد تضطر إلى تغيير مساراتها لتجنب المناطق المتضررة بالتلوث؛ ما يزيد من وقت الرحلات وتكاليف الوقود.

سادسًا: تأثيرات الصيد الجائر:

1. استنزاف الثروة السمكية والموارد البحريّة الأخرى، وهذا يمكن أن يقلل من نشاط الصيد التجاري التقليدي في المنطقة.
2. قلة الموارد البحريّة قد تؤدي إلى تقليل حركة السفن التجارية المتخصصة في نقل المنتجات البحريّة.
3. عندما تصبح الموارد البحريّة نادرة بسبب الصيد الجائر، قد تنشأ نزاعات بين الدول أو بين الصيادين المحليين والشركات الكبرى هذه النزاعات يمكن أن تؤدي إلى توترات سياسية قد تؤثر على حركة السفن وزيادة الإجراءات الأمنيّة.
4. التأثير سلبًا على البيئة البحريّة؛ ما يؤدي إلى تغيير النظم البيئية وتراجع الحياة البحريّة، وقد يؤثر هذا على حركة السفن إذا اضطرت بعض الموانئ أو مناطق الصيد إلى الإغلاق أو فرض قيود على الحركة بسبب التدهور البيئي.
5. إذا تدهورت الحياة البحريّة نتيجة الصيد الجائر، قد يتأثر قطاع السياحة في بعض المناطق؛ ما قد يقلل من حركة السفن السياحية والرحلات الترفيهية.

الفصل الثالث
تقييم المخاطر والتحديات وتحليل الاستبانة

تمهيد:

في ظل التحديات المتزايدة التي تواجه الأمن البحريّ في الخليج العربيّ، يعد تقييم المخاطر أداة أساسية لفهم وتقييم التهديدات المحتملة والتحديات الأمنيّة التي قد تؤثر على حركة الملاحة البحريّة، ويعتمد تحليل المخاطر على تقييم العوامل التي تهدد الأنشطة البحريّة، والتي تم ذكرها في الدراسة مثل القرصنة، أو الإرهاب، أو التوترات السياسية،

أو التغيرات المناخية أو بقية التحديات الأمنيّة، ويهدف هذا التحليل إلى تحديد احتمالات التهديدات ومدى تأثيرها على الملاحة البحريّة وطرق الاستجابة المناسبة.

من ناحية أخرى، يعد تحليل الاستبانة أحد الأدوات المهمة للحصول على بيانات مباشرة من المختصين والعاملين في القطاع البحريّ، ويسهم تحليل الاستبانة في جمع معلومات واقعية حول الخبرات والآراء المتعلقة بالتحديات الأمنيّة الحالية، ويمكن من خلال هذا التحليل تقييم مستوى الوعي بالمخاطر، وفعالية التدابير الأمنيّة الحالية، وأوجه القصور التي يجب معالجتها. وتساعد الاستبانة في تقديم صورة حول التهديدات والتحديات الأمنيّة وكيفية مواجهتها؛ ما يعزز القدرة على اتخاذ قرارات مدروسة لتحسين الأمن البحريّ وضمان سلامة الملاحة.

باستخدام كل من تقييم المخاطر وتحليل الاستبانة، يمكن تقديم رؤية محددة ومتخصصة حول الحالة الأمنيّة في منطقة الخليج العربيّ، مع التركيز على التحديات التي قد تؤثر على حركة الملاحة البحريّة، تم تقسيم هذا الفصل كالتالي

المبحث الأول: تقييم المخاطر والتحديات الأمنيّة في الخليج العربيّ: Risk Assessment

المبحث الثاني: تحليل وتفسير الاستبانة

المبحث الأول
تقييم المخاطر والتحديات الأمنيّة في الخليج العربيّ Risk Assessment

المطلب الأول: تقسيم العوامل وكيفية حساب النسب المئوية

لحساب وتحديد احتمالية ونسبة مئوية لتقييم المخاطر والتهديدات والتحديات التي تواجه حركة الملاحة البحريّة في الخليج العربيّ وتحديد مستوى الخطورة (منخفضة، متوسطة، مرتفعة)، وتحديد الخطر أو التهديد ووصفه والتأثير والاحتمالية والإجراءات المتخذة والمسؤول عن الإدارة، كما هو موضح بالملحق رقم (4)، تم اتباع الخطوات التالية:

أولاً: جمع البيانات والمعلومات:

1. تحديد التهديدات المحتملة: مثل القرصنة، والإرهاب البحريّ، والتهريب، والحوادث البحريّة، والتوترات السياسية.
2. جمع البيانات التاريخية: عن القرصنة، والإرهاب البحريّ، والتهريب، والحوادث البحريّة، والتوترات السياسية.
3. الاستعانة بالمصادر: تقارير الأمم المتحدة، تقارير شركات التأمين، التقارير الحكومية، تقارير المنظمات البحريّة.

ثانيًا: تحليل البيانات:

1. تحديد تكرار المهددات الأمنيّة: حساب عدد الحوادث لكل نوع من التهديدات من خلال البيانات المذكورة في الدراسة.
2. تقييم الخطورة: تقييم مدى تأثير كل مهدد أمني على حركة الملاحة البحريّة.

ثالثًا: حساب الاحتمالية والنسبة المئوية: احتمالية وقوع التهديد = (عدد الحوادث) مقسومًا على (إجمالي عدد الحوادث لجميع التهديدات) × 100.

رابعًا: تقييم درجة الخطورة: تحديد مستويات الخطورة: بناءً على الاحتمالية والتأثير، واستخدام مصفوفة تقييم المخاطر التي تربط بين احتمال وقوع التهديد ومدى تأثيره.

خامسًا: مصفوفة تقييم المخاطر والمهددات: التأثير / الاحتمالية.

1. منخفض 0 – 34%.
2. متوسطة 35% – 64%.
3. مرتفعة 65% – 100%.

المطلب الثاني

تقييم المخاطر والتهديدات الأمنيّة والملاحية في الخليج العربيّ وخليج عدن وباب المندب

1. القرصنة البحريّة: تظل القرصنة البحريّة تهديدًا كبيرًا في خليج عدن وباب المندب، خاصةً مع وجود جماعات مسلحة ومناطق غير مستقرة، بينما تكون هذه التهديدات أقل في الخليج العربيّ بسبب الإجراءات الأمنيّة الصارمة.
2. السطو المسلح: يمثل السطو المسلح تهديدًا كبيرًا في خليج عدن وباب المندب، خاصةً مع وجود جماعات مسلحة ومناطق غير مستقرة، بينما تكون هذه التهديدات أقل في الخليج العربيّ بسبب الإجراءات الأمنيّة الصارمة.
3. التهريب والأنشطة غير القانونية: يمثل التهريب والأنشطة غير القانونية تهديدًا بارزًا في خليج عدن وباب المندب بسبب ضعف الرقابة البحريّة. في الخليج العربيّ، توجد هذه الأنشطة ولكن بنسب أقل.
4. المتسللون والهجرة غير الشرعية: يمثل التسلل والهجرة غير الشرعية تهديدًا متزايدًا في الخليج العربيّ، وتوجد هذه الأنشطة ولكن بنسب أقل في خليج عدن وباب المندب بسبب ضعف الرقابة البحريّة.

5. الإرهاب البحريّ: يُعد الإرهاب البحريّ تهديدًا ملحوظًا، خاصةً في خليج عدن وباب المندب؛ حيث تنشط الجماعات الإرهابية. في الخليج العربيّ، تبقى هذه التهديدات موجودة ولكنها أقل بفضل التعاون الأمني الإقليمي والدولي.
6. الحوادث البحريّة: الحوادث البحريّة في الخليج العربيّ ذات تأثير منخفض ولكن احتماليتها كبيرة نسبة لازدياد وكثافة حركة المرور. في خليج عدن وباب المندب ومع ازدياد حركة السفن ترتفع نسبة التأثير والاحتمالية.
7. المعوقات الإدارية والتقنية للأمن البحريّ: يمثل تحديث وتطوير البنية التحتية والأنظمة الحديثة وتبسيط الإجراءات الإدارية في الخليج العربيّ تأثيرًا منخفضًا واحتمالية متوسطة نسبة للإمكانيات المتوفرة لدول الخليج، وتزيد نسبة تأثير التهديد والاحتمالية في خليج عدن وباب المندب.
8. التغيرات المناخية والظروف الجوية القاسية: تؤثر التغيرات المناخية والظروف الجوية القاسية على سلامة الملاحة؛ ما يزيد من مخاطر الحوادث البحريّة، خاصة في الخليج العربيّ.
9. التوترات السياسية والنزاعات المسلحة: التوترات السياسية في الخليج العربيّ، مثل النزاعات بين دول المنطقة، تؤثر على الأمن الملاحي. في خليج عدن وباب المندب، وتزيد النزاعات المسلحة في اليمن من المخاطر الأمنيّة.
10. التلوث البحريّ: يمثل التلوث البحريّ تهديدًا كبيرًا في الخليج العربيّ نظرًا لكثافة حركة السفن وتكرار حوادث التسرب النفطي، بينما يكون التهديد أقل قليلًا في خليج عدن وباب المندب، لكنه لا يزال ملحوظًا.
11. الطائرات المسيرة والزوارق المسيرة: كمهدد أمني بحريّ ناشئ يعد استخدام الطائرات والزوارق المسيرة منخفض التأثير ومتوسط الاحتمالية في الخليج العربيّ وفي خليج عدن وباب المندب.
12. الأمن السيبراني والهجمات الإلكترونية على السفن: تزايدت المخاطر المتعلقة بالأمن السيبراني مع تطور التكنولوجيا واستخدام الأنظمة الرقمية في إدارة السفن والموانئ. هذه التهديدات موجودة ولكنها أقل نسبيًا مقارنة بالتهديدات التقليدية.
13. الصيد الجائر: تأثيرات الصيد الجائر عالية في الخليج العربيّ وخليج عدن، واحتمالية حدوثها متوسطة في الخليج العربيّ، واحتمالية مرتفعة في خليج عدن وباب المندب بسبب نقص التنظيم والمراقبة الصارمة.

التقييم الشامل للمخاطر والمهددات الأمنيّة:

1. الخليج العربيّ: التأثير متوسط بنسبة 48 % – الاحتمالية متوسطة وتميل نحو المرتفعة بنسبة 63 %.
2. خليج عدن وباب المندب: التأثير متوسط ويميل نحو الارتفاع بنسبة 62 % – الاحتمالية مرتفعة 73 %.

نتيجة التقييم الشامل للمخاطر والمهددات الأمنيّة:

من الواضح أن خليج عدن وباب المندب يواجهان مخاطر وتهديدات أمنيّة وملاحية أكبر مقارنة بالخليج العربيّ، ويعود ذلك إلى الأوضاع السياسية غير المستقرة، ونشاط الجماعات الإرهابية والقرصنة، والصراعات المسلحة في المنطقة. ونسبة للارتباط الجيوسياسي مع منطقة الخليج العربيّ، فتأثير هذه المهددات وبصورة واضحة يؤثر على حركة الملاحة بالخليج العربيّ، بينما يستفيد الخليج العربيّ من إجراءات أمنيّة أفضل وتعاون إقليمي ودولي قوي يقلل من المخاطر الأمنيّة والملاحية.

المبحث الثاني: تحليل وتفسير الاستبانة

المطلب الأول: تحليل البيانات الأولية

أداة الدراسة: هنالك عدة وسائل تستخدم في جمع المعلومات اللازمة عن الاستبانة موضوع الدراسة، وقد تم الاعتماد في هذا البحث على الاستبانة كأداة رئيسة لجمع المعلومات من عينة الدراسة، موضح أسئلة الاستبانة بالملحق رقم (5)، واشتملت الاستبانة على أسئلة عن البيانات الشخصية لعينة الدراسة كالنوع، والعمر، والمؤهل العلمي، والوظيفة، وسنوات الخبرة. كما اشتملت على خمسة محاور رئيسة تمثل فرضيات الدراسة، وفي هذه المحاور عدد (19) سؤالاً.

أفراد عينة الاستبانة:

1. الضباط البحريّون الملاحون والمهندسون (عسكريون – مدنيون).
2. مستشارون وخبراء ومحاضرون في العلوم البحريّة.
3. خبراء الأمن البحريّ.
4. الموظفون بالقطاع البحريّ الحكومي والخاص.

قمنا بسؤال عدد (خمسين) فردًا من أفراد العينة (أي فرد يعادل نسبة 2 %) حول قضايا ومعوقات الأمن البحريّ وتأثيرها على حركة الملاحة البحريّة في الخليج العربيّ:

الجزء الأول: المعلومات الشخصية:

أولاً: العمر:

1. أقل من 30 عامًا: 10% (5 أفراد).
2. 30-40 عامًا: 30% (15 فردًا).
3. 41-50 عامًا: 40% (20 فردًا) – غالبية المشاركين من هذه الفئة العمرية من ذوي الخبرة.
4. أكثر من 50 عامًا: 20% (10 أفراد).

ثانيًا: الجنس:

1. ذكر: 98 % (49 فردًا) – غالبية المشاركين الذكور نسبة لطبيعة ولهيمنة الذكور على هذا القطاع.
2. أنثى: 2% (فرد واحد).

ثالثًا: المستوى التعليمي

1. ثانوي: 10% (5 أفراد).
2. دبلوم: 20% (10 أفراد).
3. بكالوريوس: 50% (25 فردًا) – مستوى تعليمي جيد يعكس الحاجة إلى الخبر والمعرفة بهذا المجال.
4. دراسات عليا: 20% (10 أفراد).

رابعًا: الاسم الوظيفي

1. موظف في قطاع النقل البحريّ: 30% (15 فردًا) – الحاجة لخبرة ومعرفة العاملين في هذا المجال.
2. مسؤول في ميناء: 24% (12 فرد).
3. خبير أمني بحريّ: 26% (13 فرد) – الحاجة لخبرة ومعرفة العاملين في هذا المجال.
4. أخرى: 20% (10 أفراد).

خامسًا: سنوات الخبرة في المجال

1. أقل من 5 سنوات: 10% (5 أفراد).
2. 5-10 سنوات: 24% (12 فردًا).
3. 11-20 سنة: 40 % (20 فردًا) – خبرة متنوعة مع الحاجة لرأي أصحاب الخبرة المتوسطة إلى الطويلة.

4. أكثر من 20 سنة: 26 % (13 فردًا) – خبرة متنوعة مع الحاجة لرأي أصحاب الخبرة المتوسطة إلى الطويلة.

الجزء الثاني: القضايا الأمنيّة:

أولاً: التهديدات الأمنيّة:

1. الإرهاب البحريّ: 60 % (30 فردًا) – التهديدات الأمنيّة الأكثر شيوعًا.
2. القرصنة: 50 % (25 فردًا) – التهديدات الأمنيّة الأكثر شيوعًا.
3. التوترات السياسية: 70 % (35 فردًا) – التهديدات الأمنيّة الأكثر شيوعًا.
4. تهريب المخدرات: 40 % (20 فردًا).
5. الاتجار بالبشر: 30 % (15 فردًا).
6. تجارة الأسلحة: 34 % (17 فردًا).
7. تهريب البضائع: 46 % (23 فردًا).
8. أخرى: 10 % (5 أفراد) – الصيد الجائر – الأحوال الجوية الرديئة – التلوث البحريّ – الحوادث.

ثانيًا: مدى تأثير التهديدات الأمنيّة

1. تأثير كبير: 52 % (26 فردًا) – يرى غالبية المشاركين أن التهديدات لها تأثيرًا كبيرًا.
2. تأثير متوسط: 30 % (15 فردًا).
3. تأثير قليل: 14% (7 أفراد).
4. لا يوجد تأثير: 4 % (فردان).

ثالثًا: تأثير التوترات السياسية:

1. نعم: 72 % (36 فردًا) – غالبية المشاركين تشير إلى أن التوترات السياسية تزيد من التهديدات الأمنيّة.
2. لا: 14% (7 أفراد).
3. غير متأكد: 14% (7 أفراد).

الجزء الثالث: المعوقات التقنية والإدارية

أولاً: المعوقات التقنية:

1. ضعف البنية التحتية: 50 % (25 فردًا).
2. نقص التقنيات الحديثة: 60 % (30 فردًا) – من المعوقات الرئيسة في هذا المحور.
3. عدم مواكبة الأنظمة الأمنيّة: 40 % (20 فردًا).

4. التهديدات الناشئة: 44 % (22 فردًا) – التهديد السيبراني – الذكاء الاصطناعي – الطائرات والزوارق المسيرة.
5. أخرى: 10% (5 أفراد).

ثانيًا: المعوقات الإدارية

1. التشريعات والقوانين: 54% (27 فردًا) – من المعوقات الرئيسة في هذا المحور.
2. تعقيد النظام الإداري: 40 % (20 فردًا).
3. الفساد الإداري: 34 % (17 فردًا).
4. نقص التنسيق بين الجهات المعنية: 60 % (30 فردًا).
5. أخرى: 10% (5 أفراد).

ثالثًا: كفاءة التشريعات الحالية

1. فعالة جدًا: 16% (8 افراد).
2. فعالة: 34 % (17 فردًا).
3. متوسطة الفعالية: 40 % (20 فردًا) – غالبية رأي المشاركين أشار إلى توسط الفعالية.
4. غير فعالة: 10% (5 أفراد).

الجزء الرابع: التأثيرات على حركة الملاحة البحريّة

أولاً: تأثير القضايا الأمنيّة والمعوقات

1. تأثير كبير: 52 % (26 فردًا) – تأثير القضايا والمعوقات الأمنيّة على حركة الملاحة كبير إلى متوسط التأثير.
2. تأثير متوسط: 32 % (16 فردًا) التأثير.
3. تأثير قليل: 10% (5 أفراد).
4. لا يوجد تأثير: 6 % (3 أفراد).

ثانيًا: تأخير الشحنات أو تغيير مسارات السفن

1. نعم: 60 % (30 فردًا) – غالبية المشاركين اكدت على السؤال بنعم.
2. لا: 10% (5 أفراد).
3. أحيانًا: 30 % (15 فردًا).

ثالثًا: الإجراءات لتحسين الأمن البحريّ

1. تحسين التعاون الإقليمي والدولي: 70 % (35 فردًا) – تحسين التعاون وتحديث البنية التحتية من أكثر الإجراءات تفضيلًا لدي المشاركين.
2. تحديث البنية التحتية والتقنيات: 60 % (30 فردًا).
3. تعزيز التشريعات وتطبيق القانون: 50 % (25 فردًا).
4. زيادة التدريب والتوعية الأمنيّة: 50 % (25 فردًا).
5. أخرى: 10% (5 أفراد).

الجزء الخامس: التأثيرات الأمنيّة في خليج عدن وباب المندب

أولًا: تأثير التوترات الأمنيّة في خليج عدن وباب المندب

1. تأثير كبير: 50 % (25 فردًا) – غالبية المشاركين أكد على التأثير الكبير.
2. تأثير متوسط: 36 % (18 فردًا).
3. تأثير قليل: 10% (5 أفراد).
4. لا يوجد تأثير: 6 % (3 أفراد).

ثانيًا: الوضع الأمني العام في الخليج العربيّ

1. آمن جدًا: 10% (5 أفراد).
2. آمن: 34 % (17 فردًا).
3. متوسط الأمان: 46 % (23 فردًا) – غالبية المشاركين أجاب بالوضع الأمني متوسط الأمان.
4. غير آمن: 10% (5 أفراد).

ثالثًا: الوضع الأمني العام في خليج عدن وباب المندب

1. آمن جدًا: 4 % (2 فردًا).
2. آمن: 20 % (10 أفراد).
3. متوسط الأمان: 26 % (13 فردًا).
4. غير آمن: 50 % (25 فردًا) – غالبية المشاركين أشاروا إلى أن الوضع المني غير آمن.

الجزء السادس: التوصيات والمقترحات

أولاً: اقتراحات لتحسين الأمن البحريّ

1. تحسين التعاون الإقليمي والدولي: 70% (35 فردًا) – الأكثر شيوعًا.
2. تحديث البنية التحتية والتقنيات: 60% (30 فردًا).
3. تعزيز التشريعات وتطبيق القانون: 50% (25 فردًا).
4. زيادة التدريب والتوعية الأمنيّة: 46% (23 فردًا).
5. أخرى: 10% (5 أفراد).

ثانيًا: تعليقات إضافية: اشتملت على مقترحات مثل:

1. تحسين التنسيق بين الجهات المعنية.
2. تقوية العلاقات الدولية لتعزيز الأمن.
3. زيادة التمويل لتحسين البنية التحتية.
4. تطوير برامج تدريبية لموظفي الأمن البحريّ.

المطلب الثاني: الخلاصة والنتائج والتوصيات

الخلاصة:

في ظل حركة التجارة الحرة فإن صناعة النقل البحريّ أصبحت أكثر اتساعًا، وإن اتساع الأنشطة الإجرامية والمخاطر البحريّة بما تمثله من تهديد لتلك الصناعة يتطلب مشاركة أكبر وأكثر فعالية من جانب الدول البحريّة كي تساعد على إنشاء وتطوير نظام أمن بحريّ على ظهر السفن التجارية. وللأسف تمثل السفن وسيلة انتقال مناسبة للمتسللين، كما أنها تشكل فريسة سهلة للقرصنة البحريّة والإرهاب البحريّ واستخدامها في عمليات تهريب الأسلحة والمخدرات، مع توقع لحدوث كارثة بيئية بحريّة في أي لحظة، أي تلك الأعمال الإجرامية المستهدفة للموانئ البحريّة والسفن التجارية تمثل خطرًا استراتيجيًا على حركة الملاحة البحريّة بشكل خاص وعلى صناعة النقل البحريّ بشكل عام. تستعرض هذه الدراسة «قضايا ومعوقات الأمن البحريّ وتأثيرها على حركة الملاحة البحريّة في الخليج العربيّ» التحديات الكبيرة التي تواجه أمن الملاحة البحريّة في منطقة الخليج العربيّ، والتي تعد واحدة من أكثر المناطق الحيوية بالنسبة للتجارة العالمية والنقل البحريّ. تحلل الدراسة تأثير القضايا الأمنيّة المختلفة، مثل القرصنة، النزاعات الإقليمية، والتوترات السياسية، على حركة الملاحة في هذه المنطقة الاستراتيجيّة.

تخلص الدراسة إلى أن تحديات الأمن البحريّ في الخليج العربيّ تشكل تهديدات حقيقية لحركة الملاحة البحريّة والاستقرار الاقتصادي في المنطقة. التحديات الأمنيّة، بما في ذلك النزاعات الإقليمية والقرصنة والإرهاب البحريّ والتهديدات السياسية، تؤثر بشكل كبير على سلامة وأمان حركة الملاحة البحريّة؛ ما يزيد من التكاليف ويعقد عمليات النقل البحريّ، وتؤكد الدراسة على أهمية تعزيز التعاون الدولي والإقليمي لضمان أمن الملاحة البحريّة في الخليج العربيّ، وتوصي الدراسة بضرورة تطوير استراتيجيات أمنيّة شاملة تتضمن تحسينات في التكنولوجيا البحريّة، تعزيز قدرات المراقبة، وتعزيز التنسيق بين الدول المعنية. كما تدعو إلى تعزيز التفاهم والتعاون بين الأطراف المعنية لضمان استقرار الممرات البحريّة، والذي يعد أساسيًا لاستمرارية حركة الملاحة البحريّة وازدهار صناعة النقل البحريّ.

النتائج:

1. التهديدات الأمنيّة الرئيسية: تتضمن القرصنة، والتوترات السياسية، والإرهاب البحريّ وتهريب المخدرات.
2. تأثير التوترات السياسية: التوترات السياسية تزيد من التهديدات الأمنيّة بشكل كبير.
3. المعوقات التقنية والإدارية: ضعف البنية التحتية، ونقص التقنيات الحديثة، وتعقيد النظام الإداري هي المعوقات الرئيسة لهذه الفرضية.
4. كفاءة التشريعات: تتراوح من فعالة إلى متوسطة الفعالية، مع الحاجة لتحسينها.
5. تأثير التهديدات الأمنيّة والمعوقات على حركة الملاحة: تأثير كبير، يؤدي إلى تأخير الشحنات وتغيير المسارات.
6. تأثير التوترات في خليج عدن وباب المندب: يؤثر بشكل كبير على حركة الملاحة في الخليج العربيّ.

التوصيات:

لمواجهة تحديات قضايا ومعوقات ومهددات الأمن البحريّ والتي تؤثر على حركة الملاحة البحريّة في الخليج العربيّ، اقترح التوصيات التالية:

أولاً: القرصنة البحريّة

1. تشكيل تحالفات بحريّة مع الدول الأخرى لتنفيذ دوريات مشتركة في المناطق الأكثر عرضة للقرصنة.
2. تبادل المعلومات الاستخباراتية حول نشاطات القراصنة والمناطق الخطرة.

3. استخدام أنظمة المراقبة والرصد المتقدمة، مثل الرادارات والطائرات بدون طيار، لمراقبة السفن والمناطق البحريّة الحساسة.
4. تدريب طواقم السفن على إجراءات الطوارئ وكيفية التصرف في حال وقوع هجوم قرصنة.

ثانيًا: الإرهاب البحريّ

1. تبادل المعلومات الاستخباراتية حول التهديدات الإرهابية البحريّة بين الدول.
2. تعزيز التعاون بين الأجهزة الأمنيّة والاستخباراتية لكشف ومنع العمليات الإرهابية المحتملة.
3. تنفيذ إجراءات أمان مشددة على السفن مثل التفتيش الدقيق والبروتوكولات الأمنيّة الصارمة.
4. تدريب طواقم السفن على كيفية التعامل مع التهديدات الإرهابية وإجراءات الطوارئ اللازمة.

ثالثًا: تهريب المخدرات

1. تعزيز المراقبة على الحدود البحريّة باستخدام التقنيات الحديثة مثل الطائرات بدون طيار والرادارات.
2. تعزيز التعاون بين الدول لمكافحة تهريب المخدرات عبر الحدود البحريّة.
3. تبادل المعلومات الاستخباراتية حول شبكات تهريب المخدرات ونشاطاتها.
4. تشديد القوانين والعقوبات على تهريب المخدرات وضمان تنفيذها بصرامة.
5. تنظيم حملات توعية حول خطورة تهريب المخدرات وتأثيره على المجتمع والاقتصاد.

رابعًا: تجارة البشر

1. تشديد القوانين المتعلقة بتجارة البشر وتوفير الموارد اللازمة لإنفاذها.
2. زيادة العقوبات على المتورطين في تجارة البشر لضمان الردع.
3. تعزيز التعاون وإنشاء فرق عمل بين الدول لتبادل المعلومات الاستخباراتية حول شبكات تجارة البشر.
4. تنظيم حملات توعية للمجتمع حول مخاطر تجارة البشر وكيفية التعرف على الضحايا المحتملين.
5. تقديم برامج تعليمية للموظفين الحكوميين والعاملين في مجال الهجرة والأمن حول كيفية التعامل مع حالات تجارة البشر.

خامسًا: تجارة الأسلحة

1. تطبيق قوانين صارمة على استيراد وتصدير وتداول الأسلحة.
2. إنشاء نظام رقابة وتتبع للأسلحة لضمان عدم وصولها إلى الأيدي الخطأ.

3. تعزيز التعاون وتبادل المعلومات مع المنظمات الإقليمية الدولية لمكافحة تجارة الأسلحة غير المشروعة.
4. زيادة العقوبات على الأفراد والشركات المتورطة في تهريب الأسلحة.
5. تنظيم حملات توعية حول مخاطر تجارة الأسلحة وأثرها على الأمن القومي والاستقرار الاجتماعي.
6. تشجيع المواطنين على الإبلاغ عن أي نشاط مشبوه يتعلق بتجارة الأسلحة.

سادسًا: تهريب السلع والبضائع

1. تحسين إجراءات التفتيش والرقابة في الموانئ والمطارات والمعابر الحدودية.
2. استخدام التقنيات الحديثة مثل الأشعة السينية والماسحات الضوئية لتفتيش الحاويات والشحنات.
3. تعزيز التعاون وإنشاء فرق عمل بين الدول لتبادل المعلومات حول شبكات تهريب السلع والبضائع.
4. تنظيم دورات تدريبية لموظفي الجمارك والأمن حول كيفية التعرف على عمليات التهريب والتعامل معها.
5. زيادة الوعي بين التجار والمستهلكين حول أهمية الالتزام بالقوانين التجارية وتجنب التعامل مع السلع المهربة.

سابعًا: التوترات السياسية

1. تعزيز التعاون الدولي والإقليمي لتخفيف التوترات السياسية.
2. إنشاء لجان دبلوماسية لحل النزاعات السياسية المؤثرة على الأمن البحريّ.
3. تعزيز الشراكات الأمنيّة مع الدول المجاورة والمجتمع الدولي.
4. طلب دعم المجتمع الدولي والأمم المتحدة في جهود حل النزاعات السياسية التي تؤثر على الأمن البحريّ.

ثامنًا: البنية التحتية التقنية والإدارية

1. تحديث وتطوير البنية التحتية للموانئ والمرافق البحريّة.
2. تبني التقنيات الحديثة مثل أنظمة الإدارة الذكية والسفن الذكية.
3. تبسيط الإجراءات الإدارية وتحديث الأنظمة البيروقراطية.

تاسعًا: الأمن السيبراني

1. الاستثمار في تقنيات الحماية السيبرانية المتقدمة.
2. تدريب الموظفين على كيفية التعامل مع التهديدات السيبرانية واكتشافها مبكرًا.
3. تنفيذ برامج توعية مستمرة حول الأمن السيبراني.

عاشرًا: الطائرات والزوارق المسيرة

1. تطوير ونشر أنظمة دفاعية مضادة للطائرات والزوارق المسيرة، مثل الأنظمة المضادة للطائرات بدون طيار (Counter-UAV) وأنظمة الليزر المضادة للطائرات.
2. تعزيز التعاون مع الدول الأخرى لتبادل المعلومات الاستخباراتية حول التهديدات المحتملة من الطائرات والزوارق المسيرة.
3. تحديث القوانين والتشريعات لتشمل استخدام الطائرات والزوارق المسيرة في الأعمال الإجرامية والإرهابية.
4. تدريب القوات الأمنيّة والعسكرية على كيفية التعامل مع تهديدات الطائرات والزوارق المسيرة.
5. تنظيم حملات توعية للمواطنين حول مخاطر الاستخدام غير المشروع لهذه التقنيات وكيفية الإبلاغ عن الأنشطة المشبوهة.

حادي عشر: الذكاء الاصطناعي

1. إنشاء سياسات وإجراءات قوية للأمن السيبراني لحماية الأنظمة التي تعتمد على الذكاء الاصطناعي من الهجمات.
2. استخدام تقنيات التشفير وحماية البيانات لضمان سلامة وأمن الأنظمة الذكية.
3. إنشاء هيئات تنظيمية للإشراف على استخدام تقنيات الذكاء الاصطناعي وضمان استخدامها بشكل آمن ومسؤول.
4. تبادل المعلومات والخبرات بين الدول حول كيفية التعامل مع التهديدات الأمنيّة المتعلقة بالذكاء الاصطناعي.
5. تشجيع البحث والتطوير في مجال أمن الذكاء الاصطناعي لتطوير تقنيات جديدة لمواجهة التهديدات.
6. تنظيم حملات توعية حول استخدامات الذكاء الاصطناعي والمخاطر المحتملة المرتبطة به.

ثاني عشر: التشريعات والقوانين

1. مراجعة التشريعات الحالية وتحسينها لتكون أكثر فعالية في مواجهة التهديدات الأمنيّة.
2. تطبيق العقوبات بصرامة على المخالفين لضمان الامتثال الكامل.
3. تعزيز التعاون بين الجهات التشريعية والتنفيذية لضمان فعالية التشريعات.

ثالث عشر: التهديدات الأمنيّة والمعوقات على حركة الملاحة

1. إنشاء فرق طوارئ للتعامل السريع مع الأحداث الأمنيّة.
2. تحسين نظم مراقبة حركة الملاحة وتطوير خطط استجابة للطوارئ.
3. تنسيق الجهود بين شركات الشحن والحكومات لتقليل التأثيرات السلبية.

رابع عشر: التوترات في خليج عدن وباب المندب

1. تعزيز الوجود العسكري والأمني في المناطق الحساسة مثل خليج عدن وباب المندب.
2. التعاون مع الدول المجاورة لتعزيز الأمن والاستقرار في المنطقة.
3. تبني استراتيجيات متعددة الأطراف لمواجهة التهديدات البحريّة في هذه المناطق.

خامس عشر: التغيرات المناخية والظروف الجوية القاسية

1. تصميم وتطوير بنية تحتية قادرة على تحمل الظروف الجوية القاسية مثل الفيضانات، والعواصف، وارتفاع مستوى سطح البحر.
2. تعزيز أنظمة الإنذار المبكر للكوارث الطبيعية مثل العواصف والفيضانات.
3. توفير تقنيات حديثة لرصد وتوقع الأحوال الجوية القاسية والتغيرات المناخية.
4. تطوير خطط استجابة سريعة وفعالة للطوارئ تشمل إجلاء السكان وتوفير المساعدات اللازمة.
5. تدريب فرق الطوارئ على التعامل مع الكوارث الطبيعية والظروف الجوية القاسية.
6. تبادل الخبرات والمعرفة مع الدول الأخرى حول أفضل الممارسات لمواجهة تأثيرات التغيرات المناخية.
7. دعم البحث والتطوير في مجال التقنيات الخضراء والطاقة المتجددة.
8. تنظيم حملات توعية للمجتمع حول تأثيرات التغيرات المناخية وكيفية التكيف معها.

سادس عشر: التلوث البحريّ

1. تعزيز قدرات الهيئات الوطنية المعنية بالرقابة البيئية وإنفاذ التشريعات لضمان الالتزام بالقوانين البيئية.
2. التعاون الإقليمي ومع المنظمات الدولية مثل المنظمة البحريّة الدولية (IMO) وبرنامج الأمم المتحدة للبيئة (UNEP) لتبادل الخبرات والتقنيات الحديثة في مكافحة التلوث البحريّ.
3. تركيب أنظمة الكشف المبكر عن التسربات النفطية والتلوث الكيميائي في المنشآت النفطية والموانئ.
4. وضع لوائح صارمة للتخلص من النفايات في البحر وضمان توفير مرافق كافية لمعالجة النفايات في الموانئ.
5. تنظيم حملات توعية للمجتمع حول أهمية حماية البيئة البحريّة وتأثيرات التلوث على الصحة والاقتصاد.
6. تنظيم ورش عمل ودورات تدريبية حول الإدارة المستدامة للموارد البحريّة.
7. وضع خطط طوارئ شاملة للاستجابة السريعة لحوادث التلوث البحريّ، بما في ذلك التسربات النفطية والحوادث الكيميائية.

8. تدريب فرق الاستجابة للطوارئ على تنفيذ خطط الطوارئ بكفاءة وفعالية.

سابع عشر: الحوادث البحريّة

1. تعزيز قدرات الهيئات الوطنية المعنية بالرقابة البحريّة وإنفاذ التشريعات لضمان الالتزام بقواعد السلامة.
2. تركيب أنظمة إنذار مبكر على طول السواحل والموانئ للكشف عن الحوادث البحريّة المحتملة.
3. وضع خطط شاملة للاستجابة السريعة والفعالة للحوادث البحريّة، بما في ذلك الحوادث النفطية، والحرائق، والانفجارات.
4. تدريب فرق الاستجابة للطوارئ على تنفيذ هذه الخطط بكفاءة وفعالية.
5. التعاون الإقليمي ومع المنظمات الدولية مثل المنظمة البحريّة الدولية (IMO) لتبادل الخبرات وأفضل الممارسات في مجال السلامة البحريّة.
6. المشاركة في تدريبات ومحاكاة دولية لتحسين القدرات الوطنية في الاستجابة للحوادث البحريّة.
7. تنظيم حملات توعية لأصحاب السفن والعاملين في الموانئ حول أهمية السلامة البحريّة.
8. استخدام التكنولوجيا الحديثة مثل أنظمة المراقبة الإلكترونية، وأجهزة الاستشعار لتحسين السلامة البحريّة.
9. تبني تقنيات الاتصال المتقدمة لضمان التواصل الفعال بين السفن والمراكز الساحلية.
10. دعم البحث والتطوير في مجال تقنيات الاستجابة للحوادث البحريّة، بما في ذلك الروبوتات والغواصات غير المأهولة.

ثامن عشر: الصيد الجائر

1. تعزيز وتحديث القوانين المتعلقة بالصيد الجائر، بما يشمل تحديد مواسم الصيد والكميات المسموح بصيدها.
2. ضمان تطبيق القوانين بصرامة ومراقبة الأنشطة البحريّة باستخدام التقنيات الحديثة مثل الأقمار الصناعية والطائرات بدون طيار.
3. تحديد وإنشاء محميات بحريّة لحماية الأنواع البحريّة المهددة والنظم البيئية الحساسة.
4. تشجيع الصيادين على استخدام أدوات وتقنيات صيد مستدامة، مثل الشباك الانتقائية التي تقلل من الصيد العرضي للأنواع غير المستهدفة.
5. إطلاق حملات توعية تستهدف الصيادين والجمهور العام حول مخاطر الصيد الجائر وأهمية الحفاظ على الموارد السمكية.
6. تعزيز التعاون الإقليمي ومع المنظمات الدولية مثل منظمة الأغذية والزراعة (FAO) والمنظمة البحريّة الدولية (IMO) للاستفادة من الخبرات والموارد الدولية.

الملاحق:

الملحق رقم (1)

المبادئ الأساسية التي تنفذ في حالات المتسللين

1. تمييز المتسللين عند وصولهم أو دخولهم بلاد دون وثيقة عمدًا، دخول غير شرعي وقرارات التعامل مع هذه المواقف، تكون من حث الدول في حالة وصول أو دخول المتسلل.
2. المتسلل الذي يطلب اللجوء السياسي يجب أن يعامل طبقًا لمبادئ الحماية الدولية المنصوص عليها في القانون الدولي والتشريع الوطني.
3. أصحاب السفينة أو ممتلكيها أو الربان، بالإضافة إلى هيئات الموانئ والإدارات الوطنية أن يتم التعاون بينهم قدر الإمكان في التعامل مع حالات المتسللين.
4. يجب أن يكون هنالك ترتيبات أمنيّة تطبق بطريقة علمية بواسطة أصحاب السفن أو ممتلكيها أو الربابنة بالإضافة إلى هيئات الموانئ والإدارات الوطنية، لمنع المتسللين من الصعود على السفن وتسهيل عمليه اكتشافهم قبل أن تصل السفينة إلى الميناء وأن تسمح بذلك التشريعات الوطنية والسلطات الوطنية باعتبار أن المتسلل متهرب يتلف الملكية الخاصة.
5. يجب أن يدرك جميع الأطراف أن عملية البحث الزائد تقلل من خطر التسلل، وأيضًا يمكن إنقاذ حياة المتسلل مثال (يمكن للمتسلل أن يختبئ في مكان ضار أو مغلق).
6. يجب على الدول إرجاع المتسللين إلى أوطانهم أو محل إقامتهم.
7. يجب على المتسلل العودة إلى ميناء الدولة الأصلي للصعود ويجب على الدولة قبول المتسلل وانتظار عودته وفحصه.

المصدر: الاتفاقية الدولية بشأن منع التسلل على متن السفن (بروكسل)، 1957.

ملحق رقم (2)

الاتفاقيات والمعاهدات الإقليمية والدولية

م	اسم الاتفاقية	تاريخ الاتفاقية	بيان الاتفاقية	المصادقة والتوقيع
1	الاتفاقية الدولية لسلامة الأرواح في البحار (SOLAS).	توقيعها في 1 نوفمبر 1974 ودخلت حيز التنفيذ في 25 مايو 1980.	تهدف هذه الاتفاقية إلى تحديد معايير السلامة البحريّة وتوفير إجراءات وقائية لسلامة الأرواح في البحار.	موقع ومصادق عليها من كل دول الخليج العربيّ.
2	الاتفاقية الدولية لمنع التلوث من السفن (MARPOL).	توقيعها في 2 نوفمبر 1973 ودخلت حيز التنفيذ في 2 أكتوبر 1983.	تهدف هذه الاتفاقية إلى الحد من تلوث البحار من خلال التحكم في تصريف الملوثات من السفن.	صادقت العديد من دول الخليج العربيّ على MARPOL، وهي ملزمة بها, من بين هذه الدول قطر، الإمارات، السعودية، الكويت، وعمان.
3	اتفاقية الأمم المتحدة لقانون البحار (UNCLOS).	توقيعها في 10 ديسمبر 1982 ودخلت حيز التنفيذ في 16 نوفمبر 1994.	تعتبر هذه الاتفاقية إطارًا شاملاً لحوكمة البحار والمحيطات، وتشمل جوانب عديدة مثل حرية الملاحة، المناطق الاقتصادية الخالصة، والتعاون الدولي في الأمور البحريّة.	موقع ومصادق عليها من كل دول الخليج العربيّ.
4	مدونة السلوك لمكافحة القرصنة البحريّة في غرب المحيط الهندي وخليج عدن (Djibouti Code of Conduct).	تم اعتمادها في يناير 2009.	تهدف إلى تعزيز التعاون بين الدول الساحلية لمكافحة القرصنة والسرقة المسلحة ضد السفن.	هذه المدونة تركز على التعاون الإقليمي لمكافحة القرصنة وقد شاركت فيها دول مثل الإمارات العربيّة المتحدة وعمان.

5	اتفاقية التعاون بين دول الخليج في مجال مكافحة الإرهاب والقرصنة البحريّة.	لم يتم تحديد تاريخ محدد لهذه الاتفاقية؛ لأنها تُعتبر جزءًا من التعاون المستمر بين دول مجلس التعاون الخليجي.	تركز على تعزيز التعاون الأمني والبحريّ بين دول الخليج لمواجهة التهديدات الأمنيّة المشتركة.	جميع دول مجلس التعاون الخليجي (السعودية، الإمارات، قطر، البحريّن، الكويت، عمان) تشارك في هذه الاتفاقية وتعمل على تنفيذ بنودها.
6	مذكرة التفاهم بشأن التعاون البحريّ بين دول مجلس التعاون الخليجي.	توقيعها في 27 نوفمبر 2001.	تهدف إلى تعزيز التعاون البحريّ بين دول الخليج في مجالات البحث والإنقاذ، وحماية البيئة البحريّة، ومكافحة التلوث.	جميع دول مجلس التعاون الخليجي وقعت على مذكرة التفاهم هذه وتعمل على تعزيز التعاون البحريّ بموجبها.
7	اتفاقيات التعاون البحريّ بين دول الخليج والدول الكبرى (مثل الولايات المتحدة وبريطانيا).	متجددة وتتنوع تواريخ توقيعها.	تشمل ترتيبات تعاون عسكري وأمني تهدف إلى تعزيز الأمن البحريّ في الخليج العربيّ وضمان حرية الملاحة.	تتمتع دول الخليج بعلاقات ثنائية قوية مع الدول الكبرى وتوقع بانتظام اتفاقيات تعاون بحريّ تشمل التدريب والتبادل التقني والمناورات المشترك.
8	الاتفاقية الدولية بشأن منع التسلل او المتسللين المسافرين خلسة على متن السفن (بروكسل).	تم تبني الاتفاقية من قبل المنظمة البحريّة الدولية في عام 1957.	تهدف الاتفاقية إلى وضع قواعد وإجراءات للتعامل مع المتسللين على متن السفن، وذلك لضمان سلامة السفن والركاب وللحد من المخاطر الأمنيّة.	موقع ومصادق عليها من كل دول الخليج العربيّ.
9	اتفاقيةمنظمة الأغذيةوالزراعة للأممالمتحدة (FAO)بشأنالتدابير الرامية إلىمنع الصيد غيرالقانوني وغيرالمبلغعنه وغيرالمنظم(IUU).	اعتمدتها منظمة FAO في 2001 دخلت حيز التنفيذ في 5 يونيو 2016.	مكافحة الصيد غير القانوني وغير المبلغ عنه وغير المنظم.	– صادقت عليها قطر، السعودية، الإمارات – لم تصادق عليها الكويت، عمان، البحريّن.

المصدر : https: //ar. wikipedia. org/wiki ,2024

ملحق رقم (3)

خرائط توضح العلاقة المباشرة لحركة الملاحة البحريّة بين الخليج العربيّ وخليج عدن وباب المندب

المصدر: Google maps, 2025

ملحق رقم (4)

تقييم للمخاطر والمهددات التي تواجه حركة الملاحة البحريّة في الخليج العربيّ

م	الخطر / التهديد	الوصف	التأثير	الاحتمالية	الاجراءات المتخذة	المسؤول عن الادارة
1	القرصنة البحريّة	تشكل تهديدًا كبيرًا للسفن التجارية والناقلات، الهجمات تستهدف السفن للاستيلاء على البضائع أو الحصول على فدية – عادة خارج المياه الإقليمية للدولة.	– تعطيل حركة التجارة العالمية. – زيادة تكاليف التأمين والنقل. – وتعريض حياة البحارة للخطر. – في الخليج العربيّ (40%). – في خليج عدن وباب المندب (70%).	– في الخليج العربيّ متوسطة (60%). – في خليج عدن وباب المندب مرتفعة (80%).	– تسيير دوريات بحريّة دولية. – إنشاء ممرات بحريّة آمنة. – تحسين تكنولوجيا المراقبة والرصد.	– القوات البحريّة الدولية. – المنظمة البحريّة الدوليّة (IMO). – الحكومات الوطنية.
2	السطو المسلح	هجمات مسلحة تستهدف السفن والبضائع لأغراض السرقة أو الابتزاز – عادة داخل المياه الإقليمية للدولة.	– تعريض حياة البحارة للخطر. –خسائر اقتصادية كبيرة. – تعطيل حركة الملاحة – في الخليج العربيّ (20%). – في خليج عدن وباب المندب (70%)	– في الخليج العربيّ متوسطة (60%). – في خليج عدن وباب المندب مرتفعة (80%).	– تسيير دوريات بحريّة مسلحة – تركيب أنظمة أمان متقدمة على السفن – تدريب الطواقم على إجراءات الأمن والسلامة.	– القوات البحريّة الوطنية وحرس الحدود. – الشركات المالكة للسفن. – الهيئات الأمنيّة .الوطنية والدولية.

3	جرائم التهريب	تشمل تهريب الأسلحة، المخدرات، والبضائع والسلع المحظورة.	- تعزيز الأنشطة الإجرامية - تهديد الأمن الوطني. - زيادة العنف. - في الخليج العربيّ (60%). - في خليج عدن وباب المندب (60%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب مرتفعة (80%).	- تعزيز التعاون بين وكالات إنفاذ القانون. - استخدام التكنولوجيا لرصد الشحنات. - فرض عقوبات صارمة. - التوعية الإعلامية.	- قوات حرس الحدود. - الوكالات الأمنيّة الدولية والوطنية.
4	المتسللين والهجرة غير الشرعية	تدفقات المهاجرين غير الشرعيين والمتسللين الذين يحاولون الوصول إلى دول الخليج عبر البحر.	- تحديات أمنيّة - ضغوط على الخدمات الاجتماعية والاقتصادية. - مخاطر صحية - في الخليج العربيّ (65%). - في خليج عدن وباب المندب (50%).	- في الخليج العربيّ مرتفعة (80%). - في خليج عدن وباب المندب متوسطة (60%)	- تعزيز دوريات الحدود البحريّة - التعاون الدولي لمكافحة الهجرة غير الشرعية - تحسين سياسات اللجوء والهجرة.	- قوات حرس السواحل. - الوكالات الدولية للهجرة.

5	الإرهاب البحريّ	استخدام الهجمات الإرهابية لاستهداف السفن والموانئ.	- إلحاق أضرار بالسفن. - تعطيل التجارة - التأثير على أمن الطاقة. - في الخليج العربيّ (50%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب مرتفعة (80%).	- تعزيز الإجراءات الأمنيّة في الموانئ - تدريب أطقم السفن على مواجهة التهديدات.	- القوات البحريّة الوطنية وحرس الحدود - التحالفات البحريّة الدولية
6	الحوادث البحريّة	تشمل تصادم السفن، جنوحها، وحوادث الغرق.	- خسائر في الأرواح. - أضرار بيئية واقتصادية. - تعطيل حركة الملاحة - في الخليج العربيّ (20%). - في خليج عدن وباب المندب (70%)	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب مرتفعة (80%).	- تعزيز إجراءات السلامة البحريّة - تحسين تقنيات الملاحة والاتصالات - التدريب المستمر للطواقم.	- السلطات البحريّة الوطنية - المنظمات الدولية - شركات التأمين البحريّ.
7	المعوقات الإدارية والتقنية للأمن البحريّ	تشمل البيروقراطية، نقص التنسيق بين الهيئات المختلفة، والقصور في البنية التحتية التكنولوجية.	- ضعف الاستجابة للأزمات. - بطء في عمليات الإنقاذ. - انخفاض كفاءة الإجراءات الأمنيّة - في الخليج العربيّ (20%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب مرتفعة (80%).	- تحسين التنسيق بين الهيئات المختلفة. - تحديث البنية التحتية التكنولوجية - التدريب المستمر.	- الحكومات الوطنية. - الهيئات التنظيمية البحريّة.

8	التغيرات المناخية والظروف الجوية القاسية	الأعاصير، العواصف الرملية، والتغيرات المناخية التي تؤثر على الملاحة البحريّة.	- تعطيل حركة السفن - التسبب في حوادث بحريّة. - إلحاق أضرار بالبنية التحتية الساحلية - في الخليج العربيّ (60%). - في خليج عدن وباب المندب (50%).	- في الخليج العربيّ مرتفعة (80%). - في خليج عدن وباب المندب متوسطة (60%)	- تطوير أنظمة الإنذار المبكر. - تحسين تصميم السفن. - تأهيل البنية التحتية لتحمل الكوارث الطبيعية.	- الحكومات الوطنية. - المنظمات الدولية مثل منظمة الأرصاد الجوية العالمية.
9	التوترات السياسية	التوترات بين الدول المطلة على الخليج العربيّ يمكن أن تؤدي إلى نزاعات مسلحة تؤثر على حركة الملاحة البحريّة.	- إغلاق الممرات المائية الهامة وتغيير المسارات - تعطيل حركة النفط والغاز والبضائع. - زيادة أسعار الطاقة العالمية. - في الخليج العربيّ (60%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب مرتفعة (80%).	-الدبلوماسية الدولية - العقوبات الاقتصادية. - تعزيز التحالفات الأمنيّة.	- الأمم المتحدة - التحالفات الدولية - التحالفات الإقليمية

10	التلوث البحريّ	التسرب النفطي والتلوث الناتج عن الأنشطة البحريّة.	- تلوث البحار - تأثيرات سلبية على الحياة البحريّة وصحة الإنسان. - تكاليف تنظيف مرتفعة. - في الخليج العربيّ (70%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب متوسطة (60%)	- تطبيق اللوائح البيئية الصارمة - تعزيز مراقبة الانبعاثات والتسربات. - برامج الاستجابة السريعة للتلوث.	- الهيئات البيئية الوطنية. - قوات حرس الحدود. - المنظمة البحريّة الدولية (IMO)
11	الطائرات المسيرة والزوارق المسيرة	استخدام الطائرات والزوارق المسيرة لأغراض هجومية أو استكشافية غير مشروعة.	- تهديد السفن والموانئ. - زيادة المخاطر الأمنيّة. - إمكانية تنفيذ هجمات دقيقة. - في الخليج العربيّ (20%). - في خليج عدن وباب المندب (20%).	- في الخليج العربيّ متوسطة (60%) - في خليج عدن وباب المندب متوسطة (60%)	- تطوير أنظمة دفاعية مضادة. - مراقبة الجو والبحر باستمرار. - التعاون الأمني الإقليمي والدولي.	- القوات البحريّة - قوات حرس الحدود. - الوكالات الأمنيّة - الشركات الخاصة المتخصصة .

12	التهديدات السبرانية والذكاء الاصطناعي	الهجمات السبرانية التي تستهدف الأنظمة البحريّة والموانئ، واستخدام الذكاء الاصطناعي في الأنشطة الإجرامية.	- تعطيل الأنظمة التشغيلية البحريّة. - سرقة البيانات. - تهديد الأمن الوطني - في الخليج العربيّ (70%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ مرتفعة (80%). - في خليج عدن وباب المندب مرتفعة (80%).	- تعزيز الأمن السيبراني. - تطوير تكنولوجيا دفاعية متقدمة. - التدريب على مكافحة التهديدات السيبرانية.	- الحكومات الوطنية. - الشركات التكنولوجية. - الوكالات الأمنيّة.
13	الصيد الجائر	هو استغلال مفرط للموارد السمكية يتجاوز القدرة الطبيعية للأنواع البحريّة على التكاثر والتجدد، مما يؤدي إلى استنزاف الأرصدة السمكية وانقراض بعض الأنواع.	- تأثير سالب على البيئة البحريّة. - تعطيل حركة الملاحة البحريّة. - تأثير اقتصادي بزيادة تكاليف التأمين. - في الخليج العربيّ (70%). - في خليج عدن وباب المندب (70%).	- في الخليج العربيّ (50%). - في خليج عدن وباب المندب مرتفعة (70%).	- تنظيم الصيد - انشاء محميات بحريّة. - التوعية بالمحافظة على الأنواع النادرة. - تعزيز التعاون الإقليمي والدولي لمراقبة وتنظيم الصيد والممارسات غير القانونية.	- الجهات الحكومية: وزارات البيئة والزراعة والموارد البحريّة. - المنظمات الدولية: المنظمة الدولية لحماية الحياة البحريّة، ومنظمات الأمم المتحدة المختصة. - المنظمات غير الحكومية: الجمعيات البيئية والمنظمات المعنية بحماية البيئة البحريّة.

المصدر: إعداد الباحثان، 2024م.

ملحق رقم (5)

استبانة الدراسة

بسم اللّه الرحمن الرحيم

السيد / .....

..... (كتابة الاسم اختياري)

السلام عليكم ورحمة اللّه وبركاته

استبانة لأغراض دراسة علمية بعنوان:

التحديات الأمنيّة التي تواجه الأمن البحريّ في الخليج العربيّ وتأثيرها وانعكاساتها على حركة الملاحة البحريّة

عام:

1. يجرى هذا الاستبانة لأغراض البحث العلمي فقط، وليس لأي أغراض أخرى.
2. نؤكد لك أن جميع الإجابات سوف تستخدم بسرية تامة ومهنية.
3. سنعتمد في هذه الدراسة على التحليل النوعي (Qualitative Analysis)؛ لأن طرق الحصول على البيانات تتم عن طريق الاختيار العشوائي للعينات (Random Sampling).

مع خالص الشكر والتقدير

المصدر: إعداد الباحثين، 2024م.

الجزء الأول: المعلومات الشخصية

1. العمر:
   - أقل من 30 عامًا
   - 30–40 عامًا
   - 41–50 عامًا
   - أكثر من 50 عامًا

2. الجنس:
   - ذكر
   - أنثى

3. المستوى التعليمي:
   - ثانوي
   - دبلوم
   - بكالوريوس
   - دراسات عليا

4. الاسم الوظيفي:
   - موظف في قطاع النقل البحريّ
   - مسؤول في ميناء
   - خبير أمني بحريّ
   - أخرى (يرجى التحديد: .....)

5. سنوات الخبرة في المجال:
   - أقل من 5 سنوات
   - 5–10 سنوات
   - 11–20 سنة
   - أكثر من 20 سنة

الجزء الثاني: القضايا الأمنيّة

1. ما أهم التهديدات الأمنيّة التي تواجهها حركة الملاحة البحريّة في الخليج العربيّ؟ (يمكن تحديد أكثر من خيار)
   - الإرهاب البحريّ
   - القرصنة
   - التوترات السياسية
   - تهريب المخدرات
   - الاتجار بالبشر
   - تجارة الأسلحة
   - تهريب البضائع
   - أخرى (يرجى التحديد: .....)

2. إلى أي مدى تؤثر التهديدات الأمنيّة على حركة الملاحة البحريّة؟
   - تأثير كبير
   - تأثير متوسط
   - تأثير قليل
   - لا يوجد تأثير

3. هل تعتقد أن التوترات السياسية في المنطقة تزيد من التهديدات الأمنيّة البحريّة؟
   - نعم
   - لا
   - غير متأكد

الجزء الثالث: المعوقات التقنية والإدارية

1. ما المعوقات التقنية التي تواجه الأمن البحريّ في الخليج العربيّ؟ (يمكن تحديد أكثر من خيار)
   - ضعف البنية التحتية
   - نقص التقنيات الحديثة (تكنولوجيا الاتصالات والمعلومات)
   - عدم مواكبة الأنظمة الأمنيّة
   - التهديدات الناشئة (الطائرات المسيرة – الزوارق المسيرة – الجرائم السبرانية – الذكاء الاصطناعي)
   - أخرى (يرجى التحديد: .....)

2. ما المعوقات الإدارية التي تؤثر على الأمن البحريّ؟ (يمكن تحديد أكثر من خيار)
   - التشريعات والقوانين
   - تعقيد النظام الإداري
   - الفساد الإداري
   - نقص التنسيق بين الجهات المعنية
   - أخرى (يرجى التحديد: .....)

3. كيف تقيم كفاءة التشريعات الحالية المتعلقة بالأمن البحريّ في الخليج العربيّ؟
   - فعالة جدًا
   - فعالة
   - متوسطة الفعالية
   - غير فعالة

الجزء الرابع: التأثيرات على حركة الملاحة البحريّة

1. إلى أي مدى تؤثر القضايا الأمنيّة والمعوقات التقنية والإدارية على حركة الملاحة البحريّة؟
   - تأثير كبير
   - تأثير متوسط
   - تأثير قليل
   - لا يوجد تأثير

2. هل تتسبب التهديدات الأمنيّة في تأخير الشحنات أو تغيير مسارات السفن؟
   - نعم
   - لا
   - أحيانًا

3. ما الإجراءات التي تعتقد أنها يمكن أن تحسن من الأمن البحريّ في الخليج العربيّ؟ (يمكن تحديد أكثر من خيار)
   - تحسين التعاون الإقليمي والدولي
   - تحديث البنية التحتية والتقنيات
   - تعزيز التشريعات وتطبيق القانون
   - زيادة التدريب والتوعية الأمنيّة
   - أخرى (يرجى التحديد: .....)

الجزء الخامس: التأثيرات الأمنيّة في خليج عدن وباب المندب على حركة الملاحة البحريّة في الخليج العربيّ

1. إلى أي مدى تؤثر التوترات الأمنيّة في خليج عدن وباب المندب على حركة الملاحة في الخليج العربيّ؟
   - تأثير كبير
   - تأثير متوسط
   - تأثير قليل
   - لا يوجد تأثير

2. كيف تقيم الوضع الأمني العام لحركة الملاحة البحريّة في الخليج العربيّ؟

- آمن جدًا
- آمن
- متوسط الأمان
- غير آمن

3. كيف تقيم الوضع الأمني العام لحركة الملاحة البحريّة في خليج عدن وباب المندب؟

- آمن جدًا
- آمن
- متوسط الأمان
- غير آمن

الجزء السادس: التوصيات والمقترحات

1. ما اقتراحاتك لتحسين الأمن البحريّ في الخليج العربيّ؟

.....
.....
.....
.....
.....

2. هل لديك أي تعليقات إضافية حول القضايا والمعوقات التي تواجه الأمن البحريّ وحركة الملاحة البحريّة في الخليج العربيّ؟

.....
.....
.....
.....
.....

نشكر لك وقتك ومساهمتك القيمة في هذه الدراسة

المراجع والمصادر:

أولاً: المراجع العربيّة

- غبريال أشرف سليمان، أثر المعلومات على أمن المجتمع البحريّ، دراسة ماجستير، الأكاديمية العربيّة للعلوم والتكنولوجيا والنقل البحريّ، الإسكندرية، 2003.
- أشرف كشك، نحو استراتيجيّة متكاملة للأمن البحريّ لدول الخليج العربيّ، دراسة علمية منشورة، مجلة الشؤون العربيّة، 2021.
- الزبيدي، عبد الله محمد، أمن المضايق والممرات البحريّة في الخليج العربيّ والبحر الأحمر، دراسة علمية منشورة، دار النشر، 2022.
- السبيعي، أحمد علي، الإطارات القانونية والسياسات لتعزيز الأمن البحريّ في دول مجلس التعاون الخليجي، الأطلسي كاونسل، 2023.
- محمد، علي محمد، أثر فشل الدولة على ظاهرة القرصنة البحريّة في منطقة القرن الإفريقي، (دراسة حالة دولة الصومال الفترة من 2000م – 2020م)، دراسة علمية منشورة، مجلة جامعة البحر الأحمر،2023.
- بن عيسى حياة، التهديدات البحريّة الراهنة وجهود مكافحتها، المجلة الجزائرية للقانون البحريّ والنقل، ع 1 (2014).
- ويكبيديا، الموسوعة الحرة، تسرب النفط في حرب الخليج الثانية، 2024/8، الساعة 0800.
- محمد علي محمد، التلوث البحريّ أسبابه وآثاره وطرق مكافحته، رسالة ماجستير، الأكاديمية العسكرية العليا، كلية القيادة والأركان، اليمن، 2012.
- محمد السيد أحمد، المسؤولية المدنية عن أضرار التلوث بالزيت، الإسكندرية، دار الجامعة الجديدة، الطبعة الثانيه،2005.
- محمد أمين عامر، تلوث البيئة، دراسة علمية، القاهرة، دار الكتاب الحديث، 2003.
- متابعة ذاتية لنشرات الأرصاد الجوية، المستلمة يوميًا من منظومة درع الوطن، منذ 2019 – 2024.
- عبد الحفيظ وكمال، آليات حفظ أمن البحر الأبيض من الإرهاب البحريّ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلد 6، ع 1 (2021)، 368.
- قناة الجزيرة، تعطل ميناء الفجيرة بسبب هجوم إلكتروني، 2019.

ثانيًا: المراجع الأجنبية:

- Natalie Klein, Joanna Mossop, Donald R. Rothwell, Maritime Security, International Law and Policy Perspectives from Australia and New Zealand, Routledge, Taylor & Francis Group, 2010, 21.
- Smith, A, Piracy in the Modern World: An Analysis of Maritime Security, Journal of Maritime Studies,2018.
- Bueger, C, what is maritime security? Marine Policy, (2015) 53, 159-164.
- US Department of Energy, Annual Energy Review. Retrieved from DOE, report, 2020.
- Khalid, I, Maritime Security in the Gulf Region. Naval War College Review, (2007) 65(4), 72-90.
- UNCLOS, United Nations Convention on the Law of the Sea, 1982.
- piracy and armed Robbers: Master Guide,www.marisec.org /piracy, 9/2008.
- Djibouti Code of Conduct, 29/1/2009.
- Aviva Chomsky, How Immigration became Illegal, library of Congress, 2014.
- Khalid, I, Maritime Security in the Gulf Region, Naval War College Review, 65(4) (2012), 72-90.
- Katzman, K. The Persian Gulf States and Iran: Issues for U.S. Policy, Congressional Research Service, 8/2016.
- https://safety4sea.com/steering-with-artificial-intelligence-to-combat-maritime-piracy, 8/2024, 0900.
- CSIS Reports on Maritime Threats, https://amti.csis.org,2021.
- https://www.alarabiya.net/articles, Dust storm in Saudi Arabia, 3/2009.
- https://ar.wikipedia.org/wiki/ Jeddah floods, 2011.
- https://www.IMO.org/en/OurWork/Security/Pages/Piracy-Reports, 2010 – 2024.
- https://marocbleu.com/The impact of overfishing on fish wealth, 12/2018.
- International Maritime Bureau (IMB). (2023). “Piracy and Armed Robbery Against Ships Annual.
- https://www.arabnews.com/node/1982881/2024.
- https://safety4sea.com/steering-with-artificial-intelligence-to-combat-maritime-piracy, 8/2024.
- https://www.alhurra.com/israel-hamas-war/2024.

دور الحوار والتفاوض في إدارة التظاهرات

الدكتور/ أيمن سعد الدين عبدالرحيم
الأستاذ المشارك بقسم إدارة الشرطة - أكاديمية شرطة دبي

دور الحوار والتفاوض في إدارة التظاهرات

الدكتور/ أيمن سعد الدين عبدالرحيم
الأستاذ المشارك بقسم إدارة الشرطة – أكاديمية شرطة دبي

المُلخَّص

يحفل التاريخ بتجمعات وتظاهرات حول العالم بدأت سلمية ثم انخرطت في أعمال عنف وشغب نتيجة لعدم إدارتها بشكل جيد، وقد تحدثت كثير من الدراسات الغربيّة والعربيّة عن هذه الظاهرة التي تفشت في أغلب المجتمعات، ولدى مختلف الدول غنيها وفقيرها، وعبر مختلف الأزمنة والعصور.

وقد اهتم علم النفس الاجتماعي بسلوك البشر حين يتجمعون في أعداد كبيرة؛ حيث تلاحظ اختلاف سلوكهم في هذه الحالة عن سلوكهم في حالاتهم الفرديّة، وقد ساعدت تلك الدراسات في فهم سلوك الحشود والتنبؤ بكيفيّة استجابتهم للمواقف المختلفة أثناء التظاهرات.

وقد طرحت هذه الدراسة دور الحوار والتفاوض في إدارة التظاهرات، من خلال تجارب عمليّة أثبتت نجاحها في إدارة التظاهرات في بعض الدول الغربيّة (السويد عام 2001 – كندا عامي 2001، 2002 – بريطانيا عام 2009) وأصبح لها سجل حافل واعتراف دوليّ كنموذج للممارسة الجيدة في إدارة التظاهرات.

الكلمات المفتاحية: إدارة الحشود، سيكولوجية الحشود، الحوار، التفاوض، السمات التفاوضيّة، المهارات التفاوضيّة، التظاهرات.

.

ABSTRACT

The Role of Dialogue and Negotiation in Managing Demonstrations

PhD. Ayman Saad El-Din Abdel Rahim
Associate Professor – Department of Police Administration - Dubai Police Academy

History is filled with gatherings and demonstrations practices around the world that began peacefully and then turned into violence and riots because of the failure in management procedures. Many Western and Arab studies have focused on this phenomenon, which spread in most societies, and in various countries,rich and poor, equally, and moreover, through different times and eras.

Social psychology has been concerned with "human behaviour" when people gather in large numbers, as it is noted that mass behaviour always differs from individual behaviour. Thus, these studies have helped to understand crowd's behaviour and predicted how gathering respond to different situations during demonstrations.

This study illustrates the role of "dialogue and negotiation" in managing demonstrations, by tackling practical experiences that have proven successful in crowd management in demonstrations in some countries (Sweden in 2001 - Canada in 2001, 2002 - Britain in 2009) and has a proven track record and international recognition as a model of best practice in crowd management in demonstrations.

Keywords: Crowd management, Crowd psychology, dialogue, negotiation, negotiating characteristics, negotiation skills, demonstrations.

المقدمة:

يُعد التظاهر السلميّ[1] أحد أشكال الممارسة الديمقراطيّة؛ حيث يُعد وسيلة مهمة للتعبير عن الرأي في القضايا الاجتماعيّة والسياسيّة والاقتصاديّة والثقافيّة، وهو حقّ تكفله العديد من المواثيق الدوليّة والدساتير، وتكمن أهميّة هذا الحقّ في إبراز القضايا ذات الأهميّة بالنسبة للمجتمع.

ومع ذلك، يجب أن تتم ممارسة هذا الحقّ بشكل سلميّ وبطريقة تحترم القوانين وتحافظ على النظام العام والسلم الاجتماعيّ، دون انتهاك حقوق الآخرين أو التسبب في فوضى أو ضرر بالممتلكات العامّة أو الخاصّة.

ولتحقيق التوازن بين الحقّ في التظاهر وتحقيق الأمن تضع الحكومات قوانين وسياسات تسمح بممارسة هذا الحقّ، وفي الوقت نفسه تحافظ على الأمن العام، وذلك من خلال تطبيق إجراءات تنظيميّة تضمن سلامة المتظاهرين والمواطنين والممتلكات، وتجنب أي أعمال عنف أو شغب أو تخريب.

ولبلوغ هذا الهدف تسعى بعض الأنظمة الشرطيّة إلى فهم الجوانب السيكولوجيّة للحشود؛ حتى يتسنى تحديد الاستجابات المثلى للحفاظ على النظام والسلامة خلال التظاهرات، كما تعمل على تحقيق التواصل مع الحشود باعتباره عنصرًا حيويًّا في إدارة الحشود في التظاهرات؛ حيث تكمن أهميته في فهم المطالب والمخاوف والعمل على إيجاد حلول تلبي تلك المطالب دون المساس بالأمن العام.

مشكلة الدراسة:

قد يتخذ المسؤولون عن إدارة الحشود قرارات غير ملائمة نتيجة لعدم فهمهم لسيكولوجيّة الحشود وكيفية استجابتهم للمواقف المختلفة، وقد يؤدي ذلك إلى الفوضى أو زيادة التوتر أو التسبب في حالات خطيرة، على سبيل المثال، قد يؤدي سوء توجيه الحشود أو عدم توفير ممرات كافية لهم أو عدم الحوار والتفاوض معهم بشكل جيد إلى خلق حالة

(1) المظاهرة هي كل تجمع ثابت لأفراد أو مسيرة لهم فى مكان أو طريق عام يزيد عددهم على عشرة، بقصد التعبير سلميًا عن آرائهم أو مطالبهم أو احتجاجاتهم السياسية، أما الموكب فهو كل مسيرة لأفراد فى مكان أو طريق عام يزيد عددهم على عشرة للتعبير عن آراء أو أغراض غير سياسيّة، أما الاجتماع العام فهو كل تجمع لأفراد فى كل مكان أو محل عام أو خاص يدخله أو يستطيع دخوله أى فرد دون دعوة شخصية مسبقة

من الفوضى، وقد يؤدي ذلك في حالات التظاهر إلى خروج التظاهرات عن سلميتها، أو الوصول إلى حالة من الانفلات الأمني.

لذا فإنّ فهم سيكولوجية الحشود يساعد على التنبؤ بكيفية استجابتهم للمواقف المختلفة أثناء التظاهرات؛ حيث تشير بعض دراسات علم النفس الاجتماعي إلى أنّ الأفراد عندما يتجمعون في أعداد كبيرة قد يتغير سلوكهم بسبب التأثيرات الاجتماعيّة مثل الشعور بالأمان في وسط الحشد، أو السلوك الجمعيّ، أو الاستجابة العاطفية للمواقف؛ لذا فإنّ فهم سيكولوجيّة الحشود قد يساعد على التنبؤ بكيفيّة استجابتهم للمواقف المختلفة أثناء التظاهرات.

أهمية الدراسة:

تكمن أهمية الدراسة فيما يلي:

- تسهم في سد الفراغ البحثي في المكتبات الشرطيّة[2] حول نظريات علم النفس الاجتماعيّ الحديثة التي تهتم بفهم السلوك الإنساني داخل الحشود في التظاهرات، وكيفية تحوله من الطابع السلميّ إلى الجنوح للعنف.

- تستجلي الآثار الناجمة عن الاستخدام غير المتمايز للقوة[3] من جانب الشرطة خلال حدث ما، ومدى تأثيره على سلوك الحشود في التظاهرات.

- تطرح رؤية للتعامل مع الحشود في التظاهرات، ترتكز على تجارب عمليّة أثبتت نجاحها في إدارة الحشود في التظاهرات في بعض الدول الغربيّة (السويد عام 2001 – كندا عامي 2001، 2002 – بريطانيا عام 2009) [4] كما أصبحت نموذجًا للممارسة الجيدة في إدارة الحشود في التظاهرات في العديد من الدول.

(2) أشار المرجع التالي بشكل صريح إلى أنه توجد ثغرات واضحة في الأدبيات البحثية الحالية في هذا المجال: المرجع من العام 2009. يمكن الاستشهاد بمرجع أحدث

Challenger, Rose, et al. "Understanding crowd behaviours: Supporting evidence." Understanding Crowd Behaviours'(Crown, 2009) (2009), p. xvii.

(3) أي بدون تمييز بين من قاموا بالشغب وبين غيرهم ممن وُجدوا في الحشد.

(4) تجدر الإشارة إلى أن التجارب العلميّة التي تم تناولها قد أظهرت مدى التطور الذي حدث في سلوك المتظاهرين قبل وبعد استخدام الشرطة لأسلوب الحوار والتفاوض، وكيف تطورت النتائج من الفشل في إدارة التظاهرات إلى النجاح في إدارتها، كما تضمنت التجربة الكندية مقارنة بين أسلوب شرطة مكافحة الشغب خلال حدثين مختلفين، وكيف تطورت النتائج من الفشل في إدارة الحدث الأول إلى النجاح في إدارة الحدث الثاني.

تساؤلات الدراسة:

لهذه الدراسة عدة تساؤلات، يحاول الباحث الإجابة عليها من خلال تحليل المعلومات والبيانات المتاحة، وأهم تلك التساؤلات ما يلي

- ما أهم النظريات النفسيّة في تفسير سلوك الحشود في التظاهرات؟
- ما مفهوم كل من الحوار والتفاوض؟
- ما الفرق بين الحوار والتفاوض؟
- ما السمات والمهارات التفاوضيّة اللازمة لضابط الشرطة؟
- ما أهمية التواصل مع الحشود في التظاهرات؟
- ما النتائج المترتبة على عدم فهم سيكولوجية الحشود وكيفية استجابتهم للمواقف المختلفة؟
- هل يساعد فهم سيكولوجية الحشود وكيفية استجابتهم للمواقف المختلفة في عمليّة إدارتها.
- ما أهم التجارب الدولية في مجال إدارة الحشود في التظاهرات؟

أهداف الدراسة:

تتلخص أهداف الدراسة فيما يلي:

- التعرف على مفهومي الحوار والتفاوض باعتبارهما من الأدوات المهمة في إدارة الحشود في التظاهرات؛ حيث يسهمان في تخفيف التوترات وتوجيه الأفراد نحو سلوك يحافظ على السلامة والاستقرار.

- التعرف على السمات والمهارات التي يجب توفرها في المفاوض حتى يستطيع أن يقوم بوظيفته التفاوضيّة خلال التظاهرات على خير وجه.

- التوجيه السلمي للمتظاهرين والحفاظ على النظام والسلامة العامة خلال فعاليات الاحتجاج، وخلق بيئة آمنة وسلمية للتعبير عن الرأي دون اللجوء إلى العنف أو التوترات الكبيرة، مع الحفاظ على النظام العام.

حدود الدراسة:

- الحدود الموضوعية: تغطي الدراسة الجانب النفسي للحشود في التظاهرات، للوقوف على طبيعة السلوك الجمعي وتحديد أسبابه ودوافعه، كما تغطي الجانب الأمني في إدارة الحشود، للوقوف على أسلوب متطور للتعامل معها.

- الحدود المكانية: لم تحدد الدراسة نطاقًا مكانيًا معينًا، نظراً لعمومية الموضوع وأهميته لكل دول العالم؛ لذا سعى الباحث لدراسة خبرات بعض الدول (السويد – كندا – بريطانيا) في الاستعانة بالحوار والتفاوض في إدارة الحشود في التظاهرات حتى يتسنى الاستفادة منها.

- الحدود الزمنية: تناولت الدراسة عددًا من نماذج استخدام الحوار والتفاوض في إدارة الحشود في التظاهرات خلال القرن الحالي.

نوع الدراسة والمنهج المستخدم:

تعتمد الدراسة على المنهج الوصفي [5] الذي يهدف إلى وصف وتشخيص موضوع الدراسة والعمل على تحليل مفردات ومكونات الموضوع بهدف الوصول إلى استنتاجات وتعميمات تسهم في فهم الواقع وتطويره، كما تعتمد الدراسة على المنهج المقارن الذي يهدف إلى التعرف على دور الحوار والتفاوض في إدارة التظاهرات في عدد من الدول الغربيّة (السويد – كندا – بريطانيا).

أدوات الدراسة:

اعتمد الباحث على عدد من الأدوات الأكاديمية التي تناولت الأبعاد المختلفة لموضوع الدراسة من أهمها (المؤلفات العامة والمتخصصة – الرسائل العلميّة – البحوث والدراسات السابقة التي أعِدَّت في المجال نفسه).

خطة الدراسة :

تناول الباحث موضوع الدراسة من خلال خطة منهجية قسمها إلى مبحثين بكل منهما ثلاثة مطالب، وذلك على النحو التالي

المبحث الأول: إدارة الحشود في التظاهرات

المطلب الأول: سيكولوجية الحشود في التظاهرات

المطلب الثاني: مفهوم الحوار والتفاوض الأمني

المطلب الثالث: السمات والمهارات التفاوضيّة

المبحث الثاني: بعض التجارب الدوليّة في إدارة الحشود في التظاهرات

المطلب الأول: التجربة السويدية

المطلب الثاني: التجربة الكندية

المطلب الثالث: التجربة البريطانية

(5) ربما يفضل البعض استخدام المنهج التجريبي في مثل هذه الموضوعات، إلا أن القيام بذلك يحتاج إلى عمل مؤسسي وإمكانيات كبيرة لإجراء تجارب عمليّة في مواقف الحشود المختلفة وقياس العائد منها، وهذا بالتأكيد يتجاوز قدرات الباحث، الأمر الذي دعا الباحث لاختيار المنهجين الوصفي والمقارن للدراسة.

المبحث الأول
إدارة الحشود في التظاهرات

تُعد عمليّة إدارة الحشود من أدق وأصعب العمليات الإداريّة، فإذا كانت العمليّة الإداريّة هي مجموعة الوظائف والأنشطة التي تقوم بها المنظمة من أجل تحقيق أهدافها من خلال تحليل الأهداف ورسم السياسات والخطط المطلوبة لتنفيذها، فإدارة الحشود أعقد من ذلك بكثير، فهي عمليّة تتطلب تضافر جهود العديد من الجهات المختلفة ذات الخلفيات الإداريّة والفنيّة المتباينة لتحقيق الهدف المشترك، وحتى يتسنى لتلك الجهات رسم خططها بالشكل الأمثل؛ فمن الضروري أن تكون على دراية كاملة بعنصرين أساسيين: أولهما؛ الخصائص والسمات المميزة للأفراد محل الإدارة، وثانيهما؛ الضوابط والأسس والمبادئ الواجب مراعاتها خلال تلك العمليّة الإداريّة[6].

وتهدف عمليّة إدارة الحشود في التظاهرات إلى التوجيه السلمي للمتظاهرين والحفاظ على النظام والسلامة العامة خلال فعاليات الاحتجاج؛ حيث تسهم في خلق بيئة آمنة وسلمية للتعبير عن الرأي دون اللجوء إلى العنف أو التوترات الكبيرة، ويتطلب ذلك استراتيجيات وخطوات محددة لضمان سلامة المتظاهرين والحفاظ على النظام العام، وتعتمد هذه الخطوات على الظروف الخاصة بكل تظاهرة، وقد تتطلب تعديلات أو إضافات بناءً على السياق والمتغيرات المحيطة، ويُعد فهم سيكولوجية الحشود أمرًا مهمًّا في عمليّة إدارتها؛ حيث يساعد ذلك في التنبؤ بسلوك الحشود وفهم كيفية استجابتهم للمواقف المختلفة أثناء التظاهرات.

ويُعد الحوار والتفاوض مع الحشود من الأدوات المهمة في إدارة التظاهرات بطريقة سلمية، فهما يساهمان في تخفيف التوترات وتوجيه الأفراد نحو سلوك يحافظ على السلامة والاستقرار، ويعبّر الحوار عن عمليّة تبادل الأفكار والآراء والمعلومات بين الأفراد دون ضرورة الوصول إلى اتفاق محدد أو حلٍ معينٍ، بينما يشير التفاوض إلى عمليّة تفاوضيّة تهدف إلى الوصول إلى اتفاق أو صفقة معينة تلبي مصالح الأطراف المشاركة[7].

وتتوقف نتيجة الحوار والتفاوض على السمات والمهارات والخبرات التي يتمتع بها فريق التفاوض، ولذلك يجب الاهتمام باختيار أفراده، من حيث المكونات النفسيّة، والسمات

(6) عثمان، أحمد محمد صالح أحمد. تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود (القاهرة: رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، 2022)، 59.

(7) Stott, Clifford. "Crowd psychology and public order policing: an overview of scientific theory and evidence." Submission to the HMIC Policing of Public Protest Review Team. Liverpool: University of Liverpool, UK (2009), p.19.

الشخصيّة، والقدرات العقليّة، مع الوضع في الاعتبار أن هناك سمات شخصيّة طبيعيّة لا يمكن تعلّمها، وهناك سمات يمكن اكتسابها بالتعلّم وصقلها وتنميتها بالتدريب.

ومن هذا المنطلق، يتناول الباحث هذا المبحث "إدارة الحشود في التظاهرات" من خلال ثلاثة مطالب، يتضمن المطلب الأول التعرف على سيكولوجية الحشود في التظاهرات، ويتناول المطلب الثاني مفهوم الحوار والتفاوض الأمنيّ، ويشتمل المطلب الثالث على السمات والمهارات التفاوضيّة.

المطلب الأول: سيكولوجية الحشود في التظاهرات

اهتم علم النفس الاجتماعيّ بسلوك البشر حين يتجمعون في أعداد كبيرة؛ حيث تلاحظ اختلاف سلوكهم في هذه الحالة عن سلوكهم في حالاتهم الفرديّة، وقد حاول علماء النفس والاجتماع دراسة السلوك الجمعيّ والوقوف على أسبابه ودوافعه، وقد مرت هذه الدراسات بعدة مراحل يمثل كل منها نظرية مستقلة في تفسير سلوك الحشود، كما اهتموا بتصميم نماذج للحشد[8] لوصف سلوكياته وتحركاته[9].

وهناك العديد من النظريات والنماذج التي تفسر أو تصف سلوك الحشود، وبالرغم من أهميتها إلا أنّ الفحص المتعمق لها يتجاوز نطاق هذه الدراسة؛ لذا سوف نتناول بإيجاز نموذجي (الهوية الاجتماعية لسلوك الحشود – الهوية الاجتماعية المفصل لسلوك الحشود) في وصف سلوك الحشود لاتصالهما بموضوع دراستنا.

أولًا – نموذج الهوية الاجتماعية لسلوك الحشود:
Social Identity Model of Crowd Behavior

يفترض هذا النموذج أن لكل إنسان هوية شخصيّة تشير إلى خصائصه الفريدة التي تميزه عن غيره (تخلق حالة "أنا" في مقابل "هم")، وهوية اجتماعيّة كعضو في فئة اجتماعيّة

(8) يمثل "نموذج الحشد" نظامًا يصف سلوكيات الجماهير وتحركاتهم عبر آليات محددة مسبقًا (مثل: مجموعة من القواعد، مجموعة من الصيغ، ...)، راجع:
Quanbin Sun, A Generic Approach to Modelling Individual Behaviours in Crowd Simulation,University of Salford, School of Built and Environment (2013), p.9.

(9) يهتم "علم النفس" بدراسة سلوك الكائنات الحية، وخاصةً الإنسان، وذلك بهدف التوصل إلى فهم هذا السلوك وتفسيره والتنبؤ به والتحكم فيه، بينما يهتم "علم الاجتماع" بدراسة الحياة الاجتماعية للبشر، سواء في شكل جماعات أم مجتمعات، في حين يهتم "علم النفس الاجتماعي" بدراسة التفاعل بين الفرد والمجتمع؛ حيث يدرس سلوك الفرد في إطار اجتماعي، أي من خلال المواقف الاجتماعية التي يتفاعل فيها ومعها، ويعد "علم النفس الجماعي" أو "علم نفس الحشود" أحد فروع علم النفس الاجتماعي، وكثيرًا ما يدرس كآخر فصل من فصوله، ويهتم بدراسة سلوك الحشود
راجع: مرعي، توفيق وبلقيس، أحمد. الميسر في علم النفس الاجتماعي (عمان، دار الفرقان للنشر والتوزيع، 1984) 12؛ سرسيق، إبراهيم محمد. "سيكولوجية الجماهير في القرآن الكريم"، اللجنة الوطنية القطرية للتربية والثقافة والعلوم، مجلة التربية، ع 29 (1978): 25.

فريدة مقارنة بالفئات الأخرى (تخلق حالة "نحن" في مقابل "هم")، ويشير النموذج إلى أن الأفراد داخل الحشد لا يفقدون هويتهم ولكنهم ينتقلون ببساطة من الهوية الفرديّة إلى الهوية الاجتماعيّة المشتركة، ووفقًا لذلك، لا يفقد الأفراد السيطرة على سلوكياتهم ولكن يتم التحول من التصرف من حيث هوياتهم الفرديّة إلى التصرف من حيث هويتهم الاجتماعية المشتركة[10].

وعندما يتصرف الأفراد من حيث هوية اجتماعية معينة، فإن سلوكهم يسترشد بالمعايير والقيم والمعتقدات المصاحبة لها، وبذلك يكون الأفراد قادرين على التصرف وفقًا لهذه الهوية، وهو ما يفسر كيف تكون الجماهير قادرة على التصرف تلقائيًا بطريقة متماسكة اجتماعيًا.

ومع ذلك، فإن الأفراد في الحشود – على عكس المجموعات – لا يمتلكون عادة قواعد للتعبير عن هويتهم الاجتماعية. نتيجة لذلك، يحتاج أعضاء الحشد بدلاً من ذلك إلى استنتاج المعايير النمطية التي تحدد هوية مجموعتهم من سلوكيات أولئك الذين يُنظر إليهم على أنهم أعضاء نموذجيون في الحشد. ومع ذلك، لن يتم تبني هذه المعايير إلا إذا كانت سلوكيات هؤلاء الأعضاء متوافقة مع سمات الهويّة الاجتماعيّة للمجموعة.

ويترتب على ذلك أنّه إذا كان سلوك الجمهور يعتمد على هويته الاجتماعيّة، فإن الطريقة التي يتم بها تحديد هويته ستحدد أساس سلوك هذا الجمهور، ويُعد الفهم الشامل لسلوكيات الحشد أمرًا بالغ الأهمية لضمان إدارته بكفاءة.

وهناك الكثير من الأدلة – عبر أحداث جماعيّة متعددة في سياقات متعددة[11] – لدعم نهج الهوية الاجتماعيّة لسلوكيات الجماهير؛ ما يفترض أن أعضاء الحشد يتصرفون من حيث الهويّة الاجتماعيّة[12].

وتطبيقاً لذلك فإن الجمهور الذي يتواجد باستاد رياضي لتشجيع أحد الفرق الرياضية لا يفقد كل فرد من أفراده هويته الفرديّة، ولكنهم ينتقلون ببساطة من الهوية الفرديّة (التي تختلف من شخص إلى آخر) إلى هويتهم الاجتماعيّة المشتركة (تشجيع فريق معين)، وعندما يشجعون فريقهم فإنهم يسترشدون بالمعايير والقيم والمعتقدات المصاحبة لذلك

(10) Hogg, Michael A., and Scott Tindale, eds. Blackwell handbook of social psychology: Group processes. John Wiley & Sons (2009), p.194.

(11) Hogg, Michael A., and Scott Tindale, eds., Op.Cit, p.195.

(12) La Macchia, Stephen T., and Winnifred R. Louis. "Crowd behaviour and collective action." Understanding peace and conflict through social identity theory. Springer, Cham (2016), pp.9495-.

(أسلوب وطريقة التشجيع الخاصة بفريقهم والتي تختلف من فريق إلى آخر)، وبذلك يكون الأفراد قادرين على التصرف تلقائيًا بطريقة متماسكة اجتماعيًا.

ومن هذا المنطلق،ينبغي لمديري الحشود أن يكونوا على علم بهذا التغير في سلوك الحشود حتى يسهّل عليهم إدارتهم في المواقف المختلفة.

ثانيًا – نموذج الهويّة الاجتماعيّة المفصل لسلوك الحشود:

(ESIM) Elaborated Social Identity Model of Crowd Behavior

يُستخدم هذا النموذج لفهم سلوك الحشود؛ حيث يوضح كيفيّة تأثير الهوية الاجتماعيّة على سلوك الأفراد داخل الجماعات أو الحشود، ويركز على مفهوم الهوية الاجتماعيّة ودورها في تشكيل سلوك الفرد داخل مجموعاته الاجتماعيّة، ويتألف النموذج من عدة مراحل كما يلي:

1. **التصنيف الاجتماعيّ (Social Categorization)**: الأفراد يقومون بتصنيف أنفسهم والآخرين إلى مجموعات اجتماعية مختلفة استنادًا إلى الصفات المشتركة مثل الجنس، العرق، الديانة، الهواية، أو الانتماء الاجتماعي.
2. **التوصيف الاجتماعيّ (Social Identification)**: عندما يتم التصنيف الاجتماعي، يتعرف الأفراد بشكل أكبر مع المجموعة التي يشعرون بانتمائهم إليها ويبدؤون في اعتبار أنفسهم جزءًا من هذه المجموعة.
3. **المقارنة الاجتماعيّة (Social Comparison)**: يقارن الأفراد بين مجموعتهم والمجموعات الأخرى ويبحثون عن التفوق أو أوجه الشبه بينهم.
4. **التفاعل الاجتماعيّ (Social Interaction)**: تؤثر الهوية الاجتماعية في تفاعلات الأفراد داخل المجموعات، حيث يشعر الأفراد بالانتماء والتفاعل الإيجابي داخل مجموعاتهم.
5. **التفاعل مع البيئة الخارجيّة (Interaction with the Environment)**: الأفراد يتفاعلون مع البيئة المحيطة والتي قد تؤثر على هويتهم الاجتماعيّة وسلوكهم.

ويُظهر هذا النموذج كيف أن الهوية الاجتماعيّة والانتماء إلى مجموعة ما يمكن أن تؤثر تأثيرًا كبيرًا على سلوك الأفراد داخل الحشود أو المجموعات الاجتماعيّة، ويمكن أن تؤدي هذه الهوية إلى التفاعلات الإيجابيّة والتعاون داخل الجماعات، أو تؤدي إلى التصادم والصراعات مع المجموعات الأخرى[13].

(13) Stott, Clifford, and John Drury. "The inter-group dynamics of empowerment: A social identity model." Transforming politics. Palgrave Macmillan, London (1999), pp.3245-.

كما يهتم هذا النموذج بالتفاعل الديناميكي بين المجموعات التي تشكل أحداثًا جماعيّة، ويرى أن الحشود نادرًا ما تتجمع في عزلة، وأنّ أحداث الحشد تحدث عادةً في وجود مجموعات أخرى وغالبًا ما تكون الشرطة[14].

ويرى النموذج أن الاستخدام غير المتمايز للقوة[15] من جانب الشرطة خلال حدث ما قد يؤثر سلبًا على ديناميات الحشود[16]؛ حيث يخلق عمليات نفسية تدفعهم إلى الإخلال بالنظام العام.

ويمكن لمثل هذه العمليات أن تجذب الحشد إلى الصراع على الرغم من أن الغالبية العظمى لم يكن لديها نية مسبقة للانخراط في الفوضى، وبعبارة أخرى، لم يكن تطوير "الشغب" على نطاق واسع نتاجًا لآليات داخلية للحشد ولا عن ميول أعضاء الحشد، ولكنه أصبح ممكنًا كنتيجة لأشكال محددة من التفاعلات على مستوى المجموعة التي بدأت إلى حد كبير وبدون قصد من خلال العمليات التكتيكية للشرطة[17].

وفي تفسير ذلك، تشير إحدى الدراسات إلى أنه عندما تستجيب الشرطة للإشارات المبكرة للشغب داخل الحشد (وجود أعمال عنف من مجموعات معينة أو من قبل بعض أفراد الحشد)، وذلك بتضييق الخناق على الحشد ككل، فإن النتيجة ليست فقط إعاقة تلك المجموعات ذات النيات غير القانونية، ولكن أيضًا إعاقة المجموعات الأخرى ذات النيات القانونيّة، الأمر الذي قد يدفعها إلى الصراع الجماعي نتيجة شعور هذه المجموعات بأن أفعالها المشروعة قد أعاقها الآخرون، ومن ثم فإن القيد الشرطيّ غير المتمايز يمكن أن يتسبب في أن تصبح الجماعات التي لم تكن عازمة على الصراع في الأصل أكثر استعداداً للمواجهة، وأن تصبح أقرب إلى التجمعات الأخرى الأكثر نزاعًا في الحشد وأكثر عداءً للشرطة، ما يجعل من الصعب على الشرطة قمع أي نزاع، وعندما تستخدم الشرطة المزيد من تكتيكات التدخل ضد الحشد ككل – على سبيل المثال من خلال مختلف أشكال الفض – فإنهم سيجدون أنفسهم هدفًا لعمل الشرطة، ومن ثم سيبحثون عن أكثر الطرق فعالية لتجنب الاعتقال أو الإصابة، وقد يعني ذلك التجمع مع أعضاء الحشد الآخرين من أجل اكتساب القوة الجماعيّة[18].

---

(14) Challenger, Rose, et al. Op.Cit, p.110.

(15) أي بدون تمييز بين من قاموا بالشغب وبين غيرهم ممن وُجدوا في الحشد.

(16) ديناميات الجماعة: هو مصطلح يشير إلى نظام من السلوكيات والعمليات النفسية التي تحدث داخل مجموعة اجتماعية واحدة أو بين مجموعات اجتماعية مختلفة

(17) Stott, Clifford., Op.Cit, pp.78-.

(18) Reicher, Stephen, et al. "An integrated approach to crowd psychology and public order policing." Policing: an international journal of police strategies & management (2004), p.2.

وتشير دراسة أخرى إلى أن الحشود دائمًا ما تعتقد أنها على حق بصورة لا تخلو أحيانًا من المبالغة، وتتصور دائمًا أنها تمارس حقّها القانونيّ في الاحتجاج، وتتسيدها قناعة على التوازي ناقدة للشرطة بزعم أنها تضيق عليهم، وغالبًا ما يبلغ هذا الاعتقاد مداه في لحظات اتجاه الحشد للعنف والفوضى، ومن ثم يسهل استثارتهم بمجرد تدخل الشرطة في المجرى العادي للأمور لفرض رؤيتها بالقوة حتى لو كان تدخلها مستظلاً بصحيح القانون، فتتصاعد سلوكياتهم في اتجاه العنف والفوضى، وأحيانًا تتأثر مجموعة بسلوك مجموعة أخرى أو تتعاطف معها فيطغى مشهد العنف على الموقف ويتعاظم[19].

وقد قام بعض العلماء بدراسة سلوكيات الجمهور الإنجليزيّ في العديد من الأحداث التي وُجد بها فئات غير متجانسة من البشر (مباريات كرة قدم – احتجاجات "طلابية – عمالية" – تظاهرات سلميّة للتعبير عن الرأي – ...)، وقد وجدوا أن أغلب هذه الأعمال بدأت عقب قيام الشرطة ببعض الأفعال التي أثارت حفيظة أفراد الحشد بالكامل، الأمر الذي أدى إلى تصرفهم تصرفًا عدائيّ، وزاد مؤيدوهم من المارة والمشاهدين، وخلصوا إلى أن فعلاً واحدًا خارج السياق من الممكن أن يؤدي إلى ردود أفعال عنيفة وغير متوقعة[20].

ومن ثمّ يقترح النموذج أن تكون الشرطة على علم بالظروف التي أدت إلى وجود الحشد والنيات المشروعة لأفراده، فضلاً عن تبني تكتيكات مغايرة عند التعامل مع الحشود تعتمد على: (أ) تعزيز وتسهيل السلوك السلميّ داخل الحشد من خلال تثقيف أنفسهم حول النيات المشروعة للمشاركين التي ينطلقون منها. (ب) التعويل على تكتيكات الحوار والتواصل والتفاوض مع الحشود قبل الحدث وأثناءه وبعده. (ج) تجنب التهديد غير المتناسب أو الاستخدام غير المتمايز للقوة؛ إذ يجب أن يكون استخدام القوة في حدود القبض على الأفراد الذين تسببوا في حادثة أو اتخذوا مواقف عدوانية وعنيفة، ولا ينبغي أن تمارس على أساس افتراض أن الحشد بأكمله يشكل تهديدًا للنظام العام[21].

كما أنه لا يجب التعامل مع الحشود على أنها غير عاقلة وخطيرة؛ إذ إن ذلك سوف يدفع الشرطة إلى استخدام تكتيكات تعتمد على استخدام القوة العشوائيّة أو التهديد باستخدامها، ولكن يجب التعامل مع الحشود من منطلق عقلانيتها[22].

(19) Stott, Clifford, and John Drury. "Crowds, context and identity: Dynamic categorization processes in the poll tax riot'." Human relations 53 (2000), pp. 247.273-

(20) La Macchia, Stephen T., and Winnifred R. Louis. Op.Cit, pp. 89.104-

(21) Stott, Clifford., Op.Cit, p.2.

(22) Ibid, p.19.

المطلب الثاني : مفهوم الحوار والتفاوض الأمنيّ

الحوار والتفاوض هما نوعان من الاتصال البشريّ[23] يستخدمان لأغراض مختلفة ويختلفان في هدفهما وطبيعتهما وعناصرهما الرئيسة.

فمن حيث الهدف، يهدف الحوار إلى تبادل الآراء والأفكار والمعلومات بشكل مفتوح وصريح بين الأطراف المشاركة لتحقيق التفاهم والتواصل والاستفادة من وجهات النظر المختلفة، بينما يهدف التفاوض إلى التوصل إلى اتفاق مشترك بين الأطراف المعنية عن طريق مناقشة شروط معينة وتبادل العروض والطلبات وغالبًا ما يكون التفاوض مرتبطًا بالصفقات التجارية أو القضايا السياسيّة أو الشؤون الشخصيّة.

ومن حيث الطبيعة، يمكن أن يكون الحوار أكثر عمقًا واستمرارًا، ويتضمن الاستماع الفعّال والتفاعل البناء بين الأطراف دون الضغط للوصول إلى اتفاق نهائيّ، أما التفاوض فغالبًا ما يكون أكثر تركيزًا على الوصول إلى اتفاقٍ ملموسٍ أو حلٍ محدد لمسألة معينة، وقد يشمل ذلك تبادل العروض والتنازلات للوصولٍ إلى نقطة مشتركة.

ومن حيث العناصر الرئيسة، يتضمن الحوار الاستماع الفعّال والتعبير عن الآراء والأفكار بحرية والتركيز على التفاهم والتواصل، بينما يتضمن التفاوض تحديد المصالح والاهتمامات الخاصة بكل طرف، وطرح العروض والمطالب طرحًا منهجيًّا بهدف التوصل إلى اتفاق مقبول للجميع.

وعلى الرغم من هذه الفروقات، يمكن للحوار والتفاوض أن يتقاطعا في بعض الحالات؛ حيث يمكن أن يكون الحوار جزءًا من عمليّة التفاوض لتحقيق فهم أفضل وبناء علاقات أفضل بين الأطراف المعنية.

---

(23) يوجد عدة أنواع من الاتصال البشري التي تختلف في طرقها وأساليبها، ومن أهم هذه الأنواع:
الاتصال الشفوي: يشمل استخدام الكلام لتبادل الأفكار والمعلومات، ويتضمن الحديث المباشر في المقابلات والمؤتمرات والمحاضرات
الاتصال غير الشفوي: يشمل التواصل بدون استخدام الكلام، ويشمل مجموعة من العوامل مثل لغة الجسد، وتعبيرات الوجه، والاتصال البصري، والتواصل عبر اللمس والتماس
الاتصال الكتابي: يشمل استخدام الكتابة لتبادل الأفكار والمعلومات، مثل الرسائل النصية، والبريد الإلكتروني، والمقالات، والكتب.
الاتصال الجماعي: يشمل التفاعل والتواصل بين مجموعات من الأفراد، سواء داخل الفرق العمليّة، أم المجتمعات، أم الجماعات الاجتماعية، مثل الندوات، والاجتماعات، والحوارات الجماعيّة
الاتصال العام: يشمل الاتصال مع الجمهور العام والتواصل عبر وسائل الإعلام الجماهيرية مثل وسائل الإعلام التلفزيونية، والإذاعية، ووسائل التواصل الاجتماعي
الاتصال الداخلي: يشير إلى التواصل داخل المؤسسات والشركات بين الموظفين وإدارة الشركة.
الاتصال الحكومي: يتعلق بالتواصل والتفاعل بين الحكومات والمواطنين، ويشمل الإعلانات الحكومية، والحملات التوعوية، والندوات العامة
وتلعب جميع هذه الأنواع أدوارا مهمة في التواصل البشري وتسهم في تبادل الأفكار والمعلومات وبناء العلاقات بين الأفراد والمجتمعات

أولًا – تعريف الحوار:

الحوار في معناه الاصطلاحيّ هو "عمليّة تبادل الآراء والأفكار والمعلومات بين شخصين أو أكثر، بطريقة مفتوحة وصريحة، بهدف التفاهم والتواصل، ويتضمن الحوار الاستماع الفعّال لوجهات نظر الآخرين وتقديم الردود والتعليقات تقديمًا متبادلاً ومنطقيًا؛ ما يساهم في بناء فهم مشترك وتبادل الفهم بين الأفراد أو الجماعات"[24].

كما يعرفه البعض بأنه "حديث بين شخصين، يتحدثان فيه عن موضوع معين، ولكل منهما وجهة النظر الخاصة به، التي يحاول توضيحها للطرف الآخر، ويكون الهدف منه هو التقريب في وجهات النظر المعتمدة على العقل والعلم، بعيدًا عن أي تعصب"[25].

وتشمل عمليّة الحوار عناصر أساسية مثل الاحترام المتبادل، والصدق، والاستماع الفعّال للطرف الآخر، والتعبير عن الأفكار والآراء بشكل واضح وصريح، ويهدف الحوار إلى تعزيز التواصل البناء وتحقيق التفاهم والتقارب بين الأفراد أو الثقافات المختلفة.

ويمكن أن يكون الحوار مفيدًا في حل النزاعات، وتبادل الخبرات، وبناء العلاقات الإيجابيّة بين الأفراد والمجتمعات، وتُعد مهارات الحوار والقدرة على التواصل بفعالية من الجوانب الأساسية التي تساعد في بناء علاقات جيدة وفهم أفضل للآخرين.

وقد تطور مفهوم الحوار عبر التاريخ، ففي العصور القديمة، كان الحوار يعتبر جزءًا أساسيًا من الفلسفة والحكمة في الحضارات اليونانيّة والرومانيّة القديمة؛ حيث كانت هناك مناقشات فلسفيّة وفكريّة مكثفة بين الفلاسفة والعلماء، وفي العصور الوسطى، استمر الحوار كوسيلة لانتقال المعرفة والفكر بين الثقافات المختلفة؛ حيث كانت الجامعات والمراكز الدينيّة والفلسفيّة مراكز للنقاش والحوار، ومنذ ذلك الحين استمر الحوار كوسيلة أساسيّة للتواصل والتفاهم بين الأفراد والثقافات المختلفة في جميع أنحاء العالم، واليوم يُمارس الحوار في السياسة والدين والفن والعلوم وجميع جوانب الحياة الاجتماعيّة والثقافيّة.

وقد تطوّرت طرق الحوار عبر التاريخ، بدءًا من النقاشات الفلسفيّة القديمة إلى استخدام وسائل الاتصال الحديثة مثل الإنترنت ووسائل التواصل الاجتماعيّ للتفاعل وتبادل الأفكار والآراء في العصر الحديث.

ثانيًا – أهمية الحوار:

يُعد الحوار في حالات التظاهر من الأدوات الأساسية للحفاظ على السلم الاجتماعي وتعزيز التفاهم بين الأطراف المختلفة، وتكمن أهمية الحوار في هذه الحالات في عدة جوانب

(24) روبنز، فيليب. التفاوض فن الفوز. (القاهرة، دار الخلود للتراث، 2010)، 129.

(25) فرحات، طارق خيرت. الإنذار الأخير سيكولوجية التفاوض باستخدام الذكاء الاصطناعي. (بدون دار نشر، بدون سنة نشر)، 12.

- تقليل التوتر: يسهم الحوار في تهدئة الأوضاع المتوترة بين المتظاهرين وقوات الأمن، فعندما تكون هناك قنوات اتصال مفتوحة، يقل احتمال تصعيد الأمور إلى مواجهات عنيفة.
- منع العنف: من خلال فتح حوار مبني على الثقة والاحترام المتبادل، يمكن التوصل إلى حلول سلمية وتجنب الانزلاق نحو العنف أو الفوضى.
- فهم المطالب: يساعد الحوار السلطات على فهم أسباب التظاهر والمطالب الحقيقية للمتظاهرين؛ ما يمكنهم من اتخاذ خطوات استباقيّة أو تصحيحيّة.
- بناء الثقة: حين يشعر المتظاهرون بأن صوتهم مسموع وأن هناك نية جدية للتفاوض، يزيد ذلك من ثقتهم في المؤسسات ويقلل من احتمال أن يتحول الاحتجاج إلى عنف.
- الحفاظ على النظام العام: من خلال الحوار، يمكن الوصول إلى اتفاقيات حول كيفية التظاهر بشكل آمن ومنظم؛ ما يضمن الحفاظ على النظام العام وسلامة الجميع.
- توفير حلول مستدامة: الحوار يوفر الفرصة للوصول إلى حلول توافقية بين الطرفين بدلًا من اللجوء إلى القوة أو القمع؛ ما يؤدي إلى استقرار أطول وأعمق.

ومن ثم ، يُعد الحوار في حالات التظاهر أداة مهمَّة في إدارة الحشود والحد من المخاطر الأمنية والسياسيّة المرتبطة بها.

ثالثًا – تعريف التفاوض:

رغم أن الإنسان يمارس التفاوض ممارسة طبيعيّة وبطريقة تلقائيّة عدة مرات كل يوم، إلا أن تعريف التفاوض ينطوي على بعض الصعوبات التي تتمثل فيما يلي[26]:

- كثيرًا ما يتداخل مفهوم التفاوض – عند البعض – مع بعض المفاهيم والتصورات التي تتشابه إلى حد معين مع العمل التفاوضي، ولكنها لا تعد تفاوضًا بالمعنى الدقيق للكلمة، ومثال ذلك: الحوار، والتعاون، والتناقش،... إلخ.
- تتعدد تعريفات التفاوض بحسب الزاوية التي يُنظر إليه من خلالها، فقد يحصره البعض في الجهد الدبلوماسيّ، فتكون ممارسة عمليّة التفاوض حكرًا على الدبلوماسيين وممثلي الدول من أجل إيجاد اتفاق بين فريقين متحاربين، وقد يراه البعض الآخر وظيفة يضطلع بها القائمون على أمور التسويق؛ ما يجعل معناه قريبًا من معنى عمليّة البيع أو المساومة.
- وجود تباين كبير بين فريق الممارسين، الذين يعرفون المفاوضات بطريقة عمليّة، ولكن يفوتهم في كثير من الأحيان الجوانب النظريّة أو الإطار النظريّ لعمليّة التفاوض، وبمعنى آخر، لا يكترثون كثيرًا بالنظريات، وإنما يعدونها، إما مضيعة للوقت، وإما افتعالًا لمسائل لا أساس لها في الواقع.

(26) عبد الحليم، وليد ممدوح. آليات تنمية مهارات التفاوض لدى رجل الشرطة. (القاهرة، أكاديمية الشرطة، كلية الدراسات العليا، 2013)، 3 - 4.

وعلى الرغم من هذه الصعوبات إلا أن هناك جهوداً علميّة لوضع إطار نظري يجعل من التفاوض علمًا له أصوله وقواعده، ومن تلك التعريفات للتفاوض ما يلي:

هو "نوع من الحوار بين طرفين أو أكثر يرمي إلى التوصل لاتفاق يؤدي إلى حسم النزاع بين الأطراف، ويحقق في ذات الوقت المصالح المشتركة فيما بينهم" [27].

وعرفه آخر بأنه "نوع من الحوار أو تبادل الاقتراحات بين طرفين أو أكثر بهدف التوصل إلى اتفاق يؤدي إلى حسم قضية نزاعيه بينهم، وفي الوقت نفسه الحفاظ على المصالح المشتركة فيما بينهم" [28].

كما عرفه البعض بأنه عبارة عن "عمليّة حوار بين طرفين تربطهم مصلحة مشتركة، أو صراع فيما بينهما، ويستهدف الوصول إلى اتفاق يسهم في تحقيق أهداف طرفي التفاوض"[29].

وقد عرفته الموسوعة الدولية للعلوم الاجتماعيّة (1977) بأنه: "شكل من التفاعل تحاول فيه الحكومات والمنظمات والأفراد إدارة بعض مصالحهم العامة المتصارعة، وهو عمليّة صريحة تتعلق بمشروعات أو مقترحات مضادة" [30].

وقد عرفه القاموس الأمريكي الحديث لأعمال التفاوض في مجال الإدارة والأعمال بأنه: "عمليّة وضع الشروط أو المعايير الخاصة بالاتفاق بين طرفين أو أكثر ويمكن تحقيقها من خلال الاجتماعات والمباحثات والمداولات" [31].

ويتضح من استعراض هذه المفاهيم عن التفاوض أنها تتفق في عدة محاور رئيسة، هي[32]:

- أن التفاوض يتم في العادة بين طرفين، وقد يتسع نطاقه ليشمل أكثر من طرفين.
- التفاوض أيًا كان نوعه، وأيًا كان القائمون به، وأيًا كانت أطرافه، لا بد وأن يدور حول "قضية معينة" أو "موضوع معين" يمثل محور العمليّة التفاوضيّة وميدانها الذي يتبارز فيه المتفاوضون.
- لا تتم أي عمليّة تفاوض بدون هدف أساسي تسعى إلى تحقيقه أو الوصول إليه، وتُوضع من أجله الخطط والسياسات، وتستخدم الأدوات والتكتيكات، ومن أجله تُستنفر الهمم، وتُحفز الجهود، وتُشحذ المواهب.

(27) العبودي، محسن. نحو استراتيجية علميّة في مجال إدارة الأزمات والكوارث (القاهرة، مجلة كلية الدراسات العليا، العدد الرابع، يناير 2011)، 193.

(28) حجازي، حسني عبد العزيز رزق. إدارة التفاوض في الأزمات الأمنية (رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، 2017)، 128.

(29) ندا، محمد عبد المنعم. كيف تصبح مفاوضًا فعالًا (القاهرة، هلا للنشر والطباعة، 2006)، 14.

(30) حواش، جمال. التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة (القاهرة، بدون دار نشر، 2005)، 6.

(31) حواش، جمال. التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة ، 6.

(32) عبد الحليم، آليات تنمية مهارات التفاوض لدى رجل الشرطة، 5 - 6.

- يستهدف التفاوض التوصل إلى اتفاق يؤدي إلى حسم النزاع بين الأطراف ويحقق المصالح المشتركة فيما بينهم.

رابعًا – أهمية التفاوض في العمل الأمني:

تنشأ أهمية علم التفاوض من زاويتين أساسيتين: الأولى ضرورته، والثانية حتميته، ورغم التقارب في المعنى اللفظي بين الزاويتين إلا أنهما يمثلان معًا محور وركيزة الأهمية القصوى لعلم التفاوض[33].

فإذا نظرنا إلى الزاوية الأولى وهي ضرورته، نجد أننا نعيش عصر المفاوضات، سواء بين الأفراد، أم بين الدول، أم بين الشعوب، فكافة جوانب حياتنا هى سلسلة من المواقف التفاوضيّة؛ حيث أصبح التفاوض صفة ملازمة لضرورات الحياة.

أمَّا إذا نظرنا إلى الزاوية الثانية وهي حتميته، نجد أن علم التفاوض يستمد حتميته من كونه المَخرج أو المنفذ الوحيد لمعالجة القضية التفاوضيّة، والوصول إلى حل للمشكلة المتنازع عليها، فكل طرف من أطراف القضية التفاوضيّة لديه درجة معينة من السلطة والقوة والنفوذ، ولكنه فى الوقت نفسه ليس لديه كل السلطة أو القوة أو النفوذ لإملاء إرادته وفرضها جبريًا على الطرف الآخر، ومن ثَمَّ يصبح التفاوض هو الأسلوب الوحيد المتاح أمام أطراف القضية التفاوضيّة للوصول إلى حل لها[34].

وتبرز أهمية التفاوض في العمل الأمني في أنه يُعد أحد الآليات التي تستخدمها الشرطة في مواجهة الأزمات؛ رغبة منها في ترك مساحة للحل السلمي وتجنب اللجوء إلى المواجهة الأمنية المباشرة، وبصفة خاصة في الحالات الحرجة مثل: التظاهرات، والاعتصامات، والإضرابات، وخطف الطائرات، واحتجاز الرهائن[35].

ويعد التفاوض الأمني، من حيث المبدأ جزءًا لا يتجزأ من المنظور العملياتي لمواجهة الأزمات؛ حيث ينظر له عادة كخطة بديلة وموازية لخطط العمليات الوقائية وعمليات المواجهة، حسب طبيعة ونوع الأزمة وجدوى التفاوض من عدمه، وعلى ذلك فالحل التفاوضي قد يكون حلاً مقبولاً ومجديًا في بعض الأزمات وغير مقبول في البعض الآخر؛ لذا يعد التفاوض أحد الوسائل المتاحة للقائد الأمني للتعامل مع الأزمات، سواء في مرحلة الوقاية أم مرحلة المواجهة.

(33) الخضيري، محسن أحمد. التفاوض علم تحقيق المستحيل انطلاقًا من الممكن (القاهرة، مكتبة الأنجلو المصرية، 1988)، 9.

(34) حجازي، إدارة التفاوض في الأزمات الأمنية، 126.

(35) الرميضي، جمال سعد والشمري، محمد مرضي. "مهارات التفاوض الأمني الناجح"، المجلة العربيّة للدراسات الأمنية 1، ع 38 (2022): 21.

ومع ذلك قد يكون التفاوض مستحيلاً أو مرفوضًا في بعض الحالات؛ ما يحتم التدخل الفوري باستخدام القوة لإنهاء الوضع، ومنع استمرار وتزايد الخسائر في البشر أو المال أو السيادة الوطنية.

وللتفاوض في مواجهة الأزمات مزايا عديدة منها؛ السرعة في حل الأزمات، فضلاً عن كونه أقل تكلفة إذا ما قورن بغيره من الحلول الأخرى، كما أنه يبث روح الطمأنينة في نفوس المواطنين، ويؤكد على احترام الدولة لمواطنيها وقدرة جهاز الأمن على الاستجابة والاستيعاب لمتطلبات ومستجدات العصر من احترام حقوق الإنسان، ويحسن صورة رجل الشرطة لدى الرأي العام الداخلي والخارجي، بالإضافة إلى ما يدل عليه من حضارية وتقدم الدولة لعدم ميلها لاستخدام العنف في مواجهة مواطنيها، ويفوِّت الفرصة على المتربصين والحاقدين على الدولة من الداخل والخارج في الادعاء بأن المواجهة بالقوة تهدف إلى قمع المواطنين ومخالفة المبادئ القانونية لحقوق الإنسان[36].

كما يضمن التفاوض استمرارية الاتصال والتواصل مع الطرف الآخر، وكسب الوقت لجمع أكبر قدر من المعلومات أو استغلاله في إيجاد الحلول المناسبة، كما يمكن ممارسة التفاوض سرًا أو علنًا بعكس غيره من الوسائل الأخرى، أو الجمع بين السرية والعلانية في بعض مراحل التفاوض، فضلاً عن أنه يتيح الاحتفاظ بالتوازن بين أطراف القضية التفاوضيّة[37].

وتهدف عمليّة التفاوض إلى التقارب في وجهات النظر بين الأطراف المتنازعة أو المتصارعة، لتحقيق الفهم المشترك، بلوغًا إلى تحقيق الاتفاق في موضوع الخلاف، وعادة ما يسعى كل طرف من أطراف التفاوض إلى تحقيق مصلحته، وقد يدخل في سبيل ذلك إلى صراع مع الطرف الآخر؛ ما يؤدي إلى التوتر والقلق النفسي، والمفاوض الناجح هو الذي يسعى إلى تضييق هوة الخلاف بين الأطراف حتى تكون النتيجة مرضية للكل، وبهذا يتفادى حدوث الصدام والنتائج التي لا تحمد عقباها[38].

ويعد الإلمام بالتفاوض كعلم وفن ضرورة ملحة لرجل الأمن أيًّا كانت وظيفته وأينما كان موقعه، فمن المستحيل أن يتم تجاهل الحاجة للتفاوض ولو من وقت لآخر؛ حيث إن عدم قدرة رجل الأمن على إدارة بعض المواقف الأمنية بطريقة سليمة قد يحول بعض المواقف الأمنية العابرة التي يتعرض لها أفراد الجهاز الأمني يوميًّا إلى أزمات أمنيّة تهدد بتطورات لا يحمد عقباها.

(36) عبد الحليم، آليات تنمية مهارات التفاوض لدى رجل الشرطة، 12- 13.

(37) حجازي، إدارة التفاوض في الأزمات الأمنية، 171- 172.

(38) عنب، محمد محمد محمد. التحقيق والبحث الجنائي في إدارة الأزمات والكوارث (القاهرة، بدون ناشر، 2012)، 236.

المطلب الثالث : السمات والمهارات التفاوضيّة

تتعدد السمات والمهارات التي يجب أن تتوفر في رجل التفاوض الناجح حتى يستطيع أن يقوم بوظيفته التفاوضيّة على خير وجه، وهذه السمات والمهارات تتكامل مع بعضها البعض لتضع الإطار العام والخاص لشخصية رجل التفاوض، لتجعله قادرًا وصالحًا للقيام بعمليّة التفاوض التي تُسند إليه، ومع ذلك يجب الأخذ في الاعتبار أن كل عمليّة تفاوض تحتاج إلى سمات ومهارات معينة فيمن يقوم بها، ولعل هذا يفسر أن كل موقف تفاوضي يحتاج إلى طريقة معينة لمعالجته والتعامل معه[39].

ومن الأمور الغريبة المتعلقة بالتفاوض، أن الذكاء الحاد في حد ذاته لا يعد دليلاً على الإطلاق على مهارة الشخص في عمليّة التفاوض، وإنما المهم القدرة على عرض وجهة نظره بأسلوب مؤثر ومقنع؛ إذ لا يكفي أن يكون الحق معه حتى يكون مقنعًا للطرف الآخر، وإنما لا بد أن يكون قادرًا على تفنيد حجج الطرف الآخر بأسلوب موضوعي يتناسب مع طريقة تفكير هذا الطرف، وقدراته الإدراكية، وخلفياته الثقافية، كما أن عليه أن يعرض وجهة نظره من خلال أساليب ووسائل ملائمة، ولا يُكتفى بعمليّة توصيل المعلومات وإنما لا بد أن تكون مؤثرة عاطفيًا، وقادرة على استمالة الطرف الآخر، مع حفظ ماء وجهه[40].

ويعتقد البعض خطأً أن التظاهر بالشجاعة والتحدث بصخب واستخدام صيغة التهديد والوعيد من المهارات المهمة في المفاوضات، وإن هذه المهارات تمكّن المفاوض من الأخذ بزمام المبادرة والهجوم على الطرف الآخر في المفاوضات، ويكمن خطأ وخطورة هذا المفهوم عندما يفكر الطرف الآخر بالطريقة نفسها ويتبنى المفاهيم نفسها[41].

ويمكن القول إن العمليّة التفاوضيّة حساسة ومعقدة وليس من السهل ممارستها دون توفر بعض السمات والمهارات الضرورية التي قد تكون فطرية موجودة في المفاوض منذ ولادته، وقد تكون مكتسبة عن طريق الخبرة والتدريب المستمر[42].

أولاً ـ السمات الشخصية:

تتعلق هذه السمات بالجوانب التي ولد بها المفاوض، واستعداده الفطري، وعوامل الوراثة، وتتمحور هذه السمات في قدراته العقلية وسماته الانفعالية، والمطلوب توفرها

(39) الخضيري، محسن. تنمية المهارات التفاوضيّة (القاهرة، الدار المصرية اللبنانية، الطبعة الأولى، 1993)، 193.

(40) روبنز، التفاوض فن الفوز، 66.

(41) خلف، عبد العزيز. "مهارات التفاوض"، مجلة المدير العربي، ع 151 (2000): 79.

(42) مركز بحوث الشرطة بأكاديمية الشرطة، "علم التفاوض ودوره في مواجهة الجرائم الإرهابية .. احتجاز الرهائن"، الإصدار التاسع والستون، 2017، 72.

بدرجة عالية، حتى يمكن صقلها، وتنميتها، وتطويرها، وتطويعها لتكون أكثر ملاءمة للعمل التفاوضي، ومن أهمها ما يلي:

1- الذكاء والدهاء:

يجب أن يتحلى المفاوض بدرجة عالية من الذكاء حتى يستطيع القيام بدوره التفاوضي بنجاح، ويقصد بالذكاء هنا القدرة على الفهم السريع لما يقال وما لم يُقل وحل المشكلات الجديدة التي تتولد من خلال موقف متأزم[43]، ويرتبط إدارة الموقف التفاوضي بمدى ذكاء المفاوض في معرفة أوجه القصور والضعف لدى الطرف الآخر لاستغلالها، ومعرفة أوجه القوة لتحييدها[44]، كما يعد الدهاء أمرًا حيويًّا وضروريًّا لنجاح العمل التفاوضي[45]، والدهاء هو صفة تعبّر عن الذكاء والمرونة في التصرف والتفكير، وتشير إلى القدرة على فهم الأمور بسرعة، واتخاذ القرارات الصائبة بشأنها في اللحظات الحرجة، كما يتضمن الدهاء القدرة على التفكير الاستراتيجي والمرونة في التعامل مع الوضعيات المختلفة، ويستطيع الشخص الدهيّ فهم دوافع الناس ونياتهم، واستخدام هذا الفهم في تحقيق أهدافه بطرق ذكية ومدروسة.

2- قوة الذاكرة:

يقصد بقوة الذاكرة القدرة على تخزين واسترجاع المعلومات، ويتمثل الأداء الجيد للذاكرة في القدرة على تذكر المعلومات بشكل دقيق وفعّال، ويحتاج المفاوض إلى ذاكرة قوية؛ كي تساعده على استدعاء المعلومات المفيدة في حواره مع الأطراف المعنية[46].

3- قوة الملاحظة:

كثيرًا ما تحدث أشياء صغيرة أثناء الجلسات التفاوضيّة، وهذه الأشياء الصغيرة قد تكون بمثابة مفاتيح للقضايا التفاوضيّة وأجزائها وعناصرها أو للشخصيات المتفاوض معها، وتساعد سرعة الملاحظة على إدراك ومعرفة وتشخيص هذه الأشياء والاستفادة منها في الجلسات التفاوضيّة[47]، خاصة الإحاطة بالعوامل التي تؤثر في الطرف الآخر، فعلى سبيل المثال معرفة أن هذا الطرف يعاني من حساسية شديدة ضد التدخين أو الروائح النفاذة أو حساسية ضد الجنس الآخر أو عدم التكيف معه، ويساعد كل هذا على حسن إدارة العمليّة التفاوضيّة.

(43) حواش، التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة، 146.

(44) الوزان، السيد حلمي. التفاوض .. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا (بدون دار نشر، 2011)، 56 57-.

(45) الخضيري، تنمية المهارات التفاوضيّة، 199.

(46) حواش، التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة، 147.

(47) الوزان، التفاوض .. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا، 60.

4- **اليقظة الدائمة:**

وهي من أهم صفات المفاوض الناجح، التي بدونها لا يصلح لأن يكون مفاوضًا مهما امتلك من قدرات أو مواهب تفاوضيّة؛ حيث تمثل "اليقظة" المسار الحاكم للاستفادة من هذه القدرات وتلك المواهب.

وتعني اليقظة التفاوضيّة ضرورة وجود استعداد دائم للتفاوض في أي وقت، وفي حالة تعبئة تفاوضيّة عالية مبنية على توفر معلومات دقيقة وكافية عن الطرف الآخر، ثم تحليل سليم لهذه المعلومات والوصول منها إلى مجموعة كافية ومناسبة من المؤثرات، تكفي للحصول على استنتاجات صحيحة عن قدرات وإمكانيات هذا الطرف من ناحية، وعن نياته واتجاهاته وأهدافه من ناحية أخرى، وذلك دون أي تهويل أو تهوين بأي قناعة أو حكم مسبق مبني على تقدير مقرر من قبل[48].

5- **الإدراك الشامل والمتكامل:**

إن للقضية التفاوضيّة أجزاء وعناصر، ومن إجمالي هذه الأجزاء وتلك العناصر تتركب القضية التفاوضيّة وتتكامل عناصرها، ومن ثَمَّ فإن التعامل الجزئي مع أحد هذه الأجزاء لا بد أن يتم في إطار النظرة الشاملة والمتكاملة للقضية التفاوضيّة ككل.

ومن ثَمَّ يجب أن يتصف رجل التفاوض بالقدرة على الرؤية الشاملة والكاملة والمتكاملة للقضية التفاوضيّة ككل، حتى ولو كانت مهمته تنحصر في معالجة أحد أجزائها أو عناصرها[49].

6- **الاتزان الانفعالي والهدوء النفسي:**

يقصد بالاتزان الانفعالي القدرة على التحكم في ردود الأفعال العاطفية بطريقة تسمح بالتفكير الهادئ والتصرف بشكل مناسب في مواقف مختلفة، ويتضمن الاتزان الانفعالي للمفاوض الوعي بالمشاعر الخاصة به وبالآخرين، والقدرة على التعامل مع هذه المشاعر بشكل صحيح دون أن تؤثر سلبًا على سلوكياته وقراراته.

ويتطلب النجاح في التفاوض أن يكون لدى المفاوض قدر عال من الاتزان الانفعالي والهدوء النفسي؛ حتى يستطيع أن يتحكم في غضبه وانفعالاته، خاصة إذا تعرض للاستفزاز والإثارة من الطرف الآخر؛ وذلك حتى يستطيع اتخاذ قرارات صحيحة تساعده في تحقيق الهدف التفاوضي[50].

(48) الخضيري، تنمية المهارات التفاوضيّة، 202.

(49) الوزان، التفاوض .. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا، 59.

(50) مركز بحوث الشرطة بأكاديمية الشرطة، علم التفاوض ودوره في مواجهة الجرائم الإرهابية .. احتجاز الرهائن، 72.

7- المرونة:

المرونة هي صفة تعكس القدرة على التكيف والتعامل مع التحديات بشكل إيجابي دون فقدان الثبات أو القدرة على التحكم، وهي عكس الجمود والتصلب والتزمت الذي يُعد سببًا رئيسيًا في حدوث الأزمات[51].

وتُعد المرونة من أهم سمات المفاوض الناجح؛ حيث تسمح بتلقي وجهات نظر الآخرين والإقبال على دراستها ومحاولة فهمها، ويساعد ذلك على تلاقي الآراء في بعض نقاط النزاع وتقبل ما قد يحدث من إحباطات أثناء عمليّة التفاوض، ويمكن ذلك المفاوض من إعادة دراسة الموقف من جديد ومعرفة أسباب الفشل الذي وقع فيه والأخذ بالأساليب التي تجعله يحقق انتصارًا يتطلع إليه في الجولات المقبلة[52].

8- إجادة فن الاستماع:

يعد فن الاستماع من الفنون المهمة في نجاح العمل التفاوضي فالاستماع مصدر حيوي للحصول على البيانات والمعلومات التي يعول عليها في العمل التفاوضي، بل قد يكون المصدر الوحيد المتاح حين يتم التفاوض لأول مرة مع الطرف الآخر، دون معرفة سابقة أو سابق إعداد، وتكون بالطبع هذه العمليّة بمثابة مفاوضات تمهيدية استكشافية غرضها جمع المعلومات والبيانات والإعداد الكامل للعمليّة التفاوضيّة الرئيسة[53]، كما يعد الإصغاء من المهارات الاجتماعية الضرورية لرجل الشرطة، فكل ما يتعلق بالعمل الشرطي يتوقف على المعلومات، وتعتمد القرارات الرشيدة على وفرة وصحة هذه المعلومات[54].

9- اللباقة والكياسة:

تعد طلاقة اللسان واللباقة في إدارة الحوار التفاوضي، والكياسة في حسن اختيار الألفاظ والعبارات التي تعكس الاحترام والود والرغبة الصادقة في الوصول إلى الحل التفاوضي من أحد العوامل الرئيسة في نجاح العمل التفاوضي، فعلى سبيل المثال يمكن تغيير عادات وسلوك الطرف الآخر وإجباره على التجاوب مع المفاوض عن طريق حسن إدارة الحوار التفاوضي معه بشكل بارع إلى درجة يمكن معها أن يجعله يتحمس لقضاياه ويتبنى موقفه وينسى إلى الأبد مطالبه التي كان يزمع التفاوض أو المطالبة بها، ويدخل في ذلك قدرة المفاوض على إشاعة وإضفاء جو عام من البهجة والسرور والترحيب والتقدير والاحترام للطرف الآخر[55].

(51) حواش، التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة، 147.

(52) الوزان، التفاوض .. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا ، 56.

(53) الخضيري، التفاوض علم تحقيق المستحيل انطلاقًا من الممكن، 373.

(54) الوزان، السيد حلمي، التدريب مدخل للتنمية البشرية في الشرطة (بدون دار نشر، 2009)، 49.

(55) لخضيري، تنمية المهارات التفاوضيّة، 200.

10- **قوة وجاذبية الشخصية:**

لا بد أن يتمتع المفاوض بشخصية قوية ناضجة جذابة بحيث لا يؤدي المفاوض إلى نفور وتأفف المحيطين به أو الذين يمارسون معه العمل التفاوضي، وتعتمد قوة الشخصية على إدراك المفاوض أن الطرف الذي يتفاوض معه هو إنسان أولاً قبل كل شيء، له عيوبه وله مميزاته[56].

11- **قوة التحمل:**

يجب أن يتحلى المفاوض بقوة التحمل والصبر، بمعنى أن يدرب نفسه على أن يتحمل جهدًا وضغطًا متواصلاً لمدة كبيرة، وألا يفقد في أي لحظة من اللحظات هذه القدرة، وتنصرف أيضًا قوة التحمل إلى مدى هدوء وبرود وقوة أعصابه، وعدم إمكانية استثارته أو إفقاده تحكمه في هذه الأعصاب، وإن كان من الممكن في بعض الأحيان أن يستخدم تكتيك العصبية لإحراج الطرف الآخر، أو إعطائه معلومات معينة بطريقة معينة، بحيث يشعر أنه نجح في الحصول عليها من لحظة انفعال حقيقية، في حين تكون هذه العمليّة جزءًا من خطة متكاملة لإحكام السيطرة على هذا الخصم، بإعطائه معلومات معينة تساعد على اتخاذ قرار معين يرغب في الوصول إليه[57].

ثانيًا ـ السمات الموضوعية:

تتصل هذه السمات بمدى القدرات التفاوضيّة والمعرفية التي يحوزها المفاوض، وعادة ما يكون اكتسبها من خلال التعليم والتدريب وممارسة العمل التفاوضي[58]، ومن أهمها ما يلي:

1- **القدرة على التحليل:**

تتعلق هذه القدرة بمدى معرفة رجل التفاوض لفن التحليل العلمي للقضايا التفاوضيّة وعناصرها وعواملها، وربط الأسباب بالنتائج، وإيجاد العلاقة بين المؤثر والسبب، وبين الباعث والمحصلة، وبين الجزء والكل، ومدى الارتباط بينهما، ومقدار ونوع وطبيعة العلاقة التي تحكمها معًا، وتحكم كلٍّ منها بمفرده، وكيف يقوم المفاوض بالربط بينها للوصول إلى الهدف التفاوضي.

ومن ثَمَّ يجب على المفاوض أن تكون لديه القدرة على معرفة الاتجاهات التفاوضيّة للخصم، ونعنى بها

(56) الخضيري، تنمية المهارات التفاوضيّة، 198.

(57) المرجع السابق، 198- 199.

(58) المرجع السابق، 195.

- هل النية متجهة نحو تجميد التفاوض؟
- هل النية متجهة نحو الخداع؟
- هل النية متجهة نحو الانسحاب بهدوء؟
- هل النية متجهة نحو الانسحاب الظاهري؟
- هل النية متجهة نحو الانسحاب والتسويف؟
- هل النية متجهة نحو الحل والوصول إلى اتفاق؟

ويجب أن يعرف المفاوض كيف يبدأ في التعامل مع هذه الاتجاهات حتى يصل إلى تحقيق الأهداف التفاوضيّة، وعليه أن يحسب النتائج المتوقعة من كل بديل من البدائل السابقة، وأي الخيارات أفضل[59].

2- المعرفة القانونية:

تعد المعرفة القانونية وما يتصل بها من تعديلات من أهم أنواع المعارف اللازمة للمفاوض التي يجب أن يحوزها بشكل دائم ومستمر، وأن يحيط بالقواعد القانونية للمجتمع الذى يتفاوض فيه ونسق القيم والعادات التي تحكمه حتى تأتي نتائج مفاوضاته في إطار هذا النظام ولا تخالف أحد أحكامه، أما إذا لم تكن لديه هذه المعرفة، فإن عليه أن يستعين بأحد المتخصصين في الشؤون القانونية حتى لا يقع في أي خطأ قانوني يمكن أن يهدم جهوده التفاوضيّة.

وبالنسبة لرجل الشرطة فإن هذه المعرفة تتفاوت بحسب الفئة التي ينتمى إليها، فضابط الشرطة يُفترض فيه الإلمام الكامل بالقواعد القانونية والنظام العام في المجتمع؛ وذلك نظرًا لما يتلقاه من دراسات قانونية خلال مرحلة التعليم والتأهيل بكلية الشرطة[60].

3- المعرفة اللغوية:

يجب أن يتقن المفاوض اللغة التي تم اختيارها للتفاوض، وأن يعي جيدًا معاني الكلمات والعبارات التي يستخدمها، ويجب عليه أن يفرق جيدًا بين المعنى اللغوي للكلمة الوارد في المعاجم اللغوية، ومعناها الاصطلاحي، ومعناها الدارج بين الناس.

ويفضل دائمًا اختيار الكلمات التي لا تختلف معانيها الاصطلاحية عن معانيها اللغوية أو الدارجة، فإن كانت هناك صعوبة في تحديد المعنى العام للكلمة أو أحس المفاوض أنها قد تحدث خلاف خلال تنفيذ الاتفاقية في المستقبل فيجب إدراجها في الاتفاقية وتحديد معناها المقصود تحديدًا دقيقًا، كما يمكن الاستعانة بمترجم في حالة اختلاف لغة الطرف الآخر[61].

(59) الوزان، التفاوض.. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا ، 62.

(60) عبد الحليم، آليات تنمية مهارات التفاوض لدى رجل الشرطة، 25.

(61) الخضيري، تنمية المهارات التفاوضيّة، 196.

4- **المعرفة النفسية:**

يلزم رجل التفاوض أن يكون ملمًّا بعلم النفس وأصوله ونظرياته وقواعده حتى يستطيع أن يحدد الطبيعة والمزاج النفسي للطرف الذى يتفاوض معه، وفي الوقت نفسه يحدد الأدوات النفسية التي سوف يستخدمها في ممارسة الضغط النفسي عليه لإقناعه أو إجباره على قبول ما يعرض عليه، أو على الأقل التأثير فيه بالشكل الذي يجعله غير قادر على فرض رأيه، أو الاستمرار في التعنت والتشدد في عرض مطالبه، فضلاً عن معرفة أكثر التكتيكات التي سوف يستخدمها هذا الطرف في مفاوضاته، وتصميم وإعداد التكتيكات المضادة، والتخطيط لتنفيذها بدقة لتحقيق المكاسب التفاوضيّة[62].

5- **المعرفة الاقتصادية:**

يجب أن يتوفر لدى المفاوض قدر مناسب من المعرفة بعلم الاقتصاد؛ حتى يستطيع حساب حجم التكلفة ومقدار العائد الخاص بكل عنصر أو جزء يتم التفاوض عليه، ومن ثَمَّ يستطيع إجراء مقارنة بين إجمالي العوائد والتكاليف[63].

6- **المعرفة القياسية:**

تتصل هذه المعرفة بعلم القياس الذي يمكن من خلاله ترجمة النقاط التفاوضيّة إلى قياس كمي، وذلك حتى يستطيع المفاوض حساب أثر هذه النقاط والاستفادة من كل هذا أثناء عمليّة التفاوض مع الطرف الآخر[64].

7- **المعرفة العامة:**

تضم هذه المعرفة كافة النواحي الثقافية التي تشكل الإطار العام لثقافة المفاوض، وهناك قاعدة مهمة لرجل التفاوض، ولكل من يرغب في الوصول إلى كونه مفاوضًا ناجحًا، وهي: "أن يعرف شيء عن كل شيء، وأن يعرف كل شيء عن العمل التفاوضي الذي سوف يمارسه".

ويساعد ذلك المفاوض في الحديث بطلاقة مع الطرف الآخر ومجاراته في الاجتماعات الرسمية وغير الرسمية[65].

(62) الوزان، التفاوض .. كيف تكون مفاوضًا أمنيًا ناجحًا ومقنعًا ، 63 - 64.

(63) روبنز، التفاوض فن الفوز، 69.

(64) آندرسون، برابرة. مهارات التفاوض الاحترافي. (القاهرة، مكتبة الهلال للنشر والتوزيع، 2010)، 77.

(65) الخضيري، تنمية المهارات التفاوضيّة، 197- 198.

المبحث الثاني
بعض التجارب الدولية في إدارة الحشود في التظاهرات

ثار جدل طويل في العقدين الماضيين حول تحول سياسات وممارسات شرطة مكافحة الشغب في الدول الغربيّة من الأسلوب القائم على المواجهة الخشنة مع الحشود إلى نموذج يستند إلى فكرة نزع فتيل العنف وتسوية النزاع، والذي يعتمد على جمع المعلومات والتواصل مع المتظاهرين والحوار والتفاوض معهم، والسبب وراء هذا التحول هو التوجه العام نحو مجتمع يتمتع بالديمقراطية بشكل أكبر، وعمليّة التغيير الاجتماعي التي أنتجت مجتمعات ما بعد الحداثة[66].

ونتناول فيما يلي أهم التجارب الدولية في السيطرة على الحشود، وفقًا للاتجاهات الحديثة وما خلصت إليه دراسات علم النفس الاجتماعي في هذا الشأن.

ويتناول الباحث في هذا المبحث "بعض التجارب الدولية في إدارة الحشود في التظاهرات" من خلال ثلاثة مطالب، يتضمن المطلب الأول التجربة السويدية، ويتناول المطلب الثاني التجربة الكندية، ويشتمل المطلب الثالث على التجربة البريطانية.

المطلب الأول: التجربة السويدية

النموذج السويدي في التعامل مع التظاهرات الاحتجاجية كان تكتيكًا بديلاً أعدته السلطات سلفًا لحالات الطوارئ، وتم تجربته في ظروف طارئة فحقق نجاحًا دفع الحكومة السويدية لجعله نموذجًا أساسيًا وعممت التعامل به مع التظاهرات.

وقد ظهر هذا النموذج عام (2001) على خلفية أحداث دامية صاحبت تظاهرات للتعبير عن رفض سياسات الاتحاد الأوروبي والولايات المتحدة الأمريكية تجاه قضايا العولمة، وتزامنت مع انعقاد قمة أوروبية على الأراضي السويدية، ومع زيارة للرئيس الأمريكي جورج بوش، وقد بلغت التظاهرات (43) تظاهرة شارك فيها قرابة (50) ألف شخص، وكان التجمع الأبرز لهؤلاء المتظاهرين في حيز وسط مدينة جوتنبرج، وضم هذا التجمع حشودًا غفيرة انخرطت مجموعات منها في أعمال عنف وإتلاف للممتلكات[67]؛ ما دعا الشرطة لاعتقال عدد (459) شخصًا منهم، وقد بلغ الحدث ذروته عندما أطلقت الشرطة النار على

(66) "King, Mike. "From reactive policing to crowd management? Policing anti-globalization protest in Canada." (2014), p 40.

(67) إبراهيم، حليم أحمد محمود، "تطبيقات علم النفس الاجتماعي في تعامل الشرطة مع الاحتجاجات"، القيادة العامة لشرطة الشارقة، دورية الفكر الشرطي 24، ع 95 (أكتوبر 2015): 72 - 73.

المتظاهرين فجرح ثلاثة منهم، كما أسفرت الاشتباكات عن إصابة عدد (150) شخصًا من بينهم (50) من ضباط الشرطة[68]، واستمرت الأحداث مرشحة للتصاعد وسط مخاوف من تحولها إلى كارثة قومية.

وعلى أثر ذلك، أمرت الحكومة السويدية بتشكيل لجنة خاصة، عرفت باسم لجنة جوتنبرج، للتحقيق في الأحداث، وقد أبرز تقرير اللجنة أوجه القصور الخطيرة في تدريب الشرطة على إدارة الحشود، وفي الجوانب الفنية للعمل، كما أثبت أن ضباط الشرطة من مختلف أجهزة الشرطة طبقوا نماذج تكتيكية مختلفة، وقد أكد التقرير أهمية استخدام الحوار في التعامل مع التظاهرات[69].

وعلى ضوء التقارير التي تلقاها المسؤولون، أصدروا تكليفات بتغيير أسلوب التعامل الشرطي واللجوء للتكتيك الشرطي البديل، والذي ارتكز إلى عدد من المبادئ المهمة[70]:

- التمكين من الحقوق.
- الحوار الدائم والمستمر.
- الحوار من منطلق تبادل الأدوار.
- الاعتبار بالفروق وعدم وضع المتظاهرين في خندق واحد.
- التركيز على فكرة القيم وفكرة الدولة.

ولكي تصيغ السلطات هذا التكتيك بادرت باتخاذ الخطوات التالية:

- تغيير زي قوات الشرطة لزي أشبه ما يكون بالقوات الخاصة.
- إصدار تعليمات مشددة لقوات الشرطة بالتعامل بمرونة مع المتظاهرين.
- التركيز على الالتزام بالزي المقرر للقوات مع اتخاذ متطلبات الحماية الشخصية مثل الدروع والخوذات والهراوات.
- توفير بعض أوجه الدعم اللوجيستي الذي يكفل للقوات أن تكون خفيفة الحركة وسريعة الانتقال.
- تنظيم القوات في شكل مجموعات تضم كل مجموعة في داخلها: قوات نظامية، مجموعة قبض، مجموعة نقل المقبوض عليهم، فريق منوط به التواصل الفعال مع الآخرين بالحوار.

(68) Stott, Clifford., Op.Cit, p.17.

(69) Holgersson, Stefan. Dialogue police: experiences, observations and opportunities. National Police Board (2010), p.15.

(70) Waddington, David P. "From Iron Fists to Bunches of Fives: A Critical Reflection on Dialogue (or Liaison) Approaches to Policing Political Protest." Special Issue 1 Eur. Police Sci. & Res. Bull. (2013), p.3132-.

- تحديد شخصين من قوات الشرطة بزي محدد مكتوب عليه "ضباط اتصال"، وتكون مهمتهما محددة في التواصل وإجراء حوارات مع المحتجين بدون قوة تأمين ظاهرة، ومن ثمّ دون تنفيذ قواعد الأمن الشخصي المقررة، وكان الهدف من الحوار مع المتظاهرين محدد من البداية: "تمكينهم من حقوقهم المشروعة في التظاهر، وتخفيف حالة الصراع والمواجهة مع القوات، وتوعية الحشود بأهمية قيام مجموعات منهم بدور الشرطة الداخلية لمنع أية محاولة للإخلال بالقانون، ومنها حالات العنف والفوضى، وتوعية المتظاهرين بضوابط الاحتجاج بأساليب الشرح والمناقشة والتفاوض.

تم إسناد مهمة الحوار مع المتظاهرين لضباط من الرتب الوسطى، وكان المقصد من ذلك ألا يكون القائد نفسه هو القائم بالتفاوض؛ لكي تترك للقيادة فرصة لاتخاذ القرارات وفق آليات دقيقة[71].

وقد تضمن التكتيك إيضاحات حول ضوابط الحوار المأمول، فيما يلي:

- تحذير الضباط المنوط بهم الحوار من مغبة توجيه الحشود للانصراف، خشية شعورهم بالخديعة أو اعتقادهم بوجود نيات لإهمال حقوقهم في الاحتجاج، كما تنبه عليهم بالتأكيد على مرجعية حقوق الإنسان كأساس للحوار.
- تم توجيه الضباط المنوط بهم الحوار لإظهار قناعتهم بأهمية التمكين من الحق في الاحتجاج والحق في التعبير والحق في الاجتماع، والعمل على حشد تأييد المتظاهرين للوصول لحالة الاستقرار والتي تتطلب تخفيف المواجهة بين ثلاثة أطراف (المتظاهرين، خصوم المتظاهرين، الشرطة).
- إتاحة مساحات للضباط المنوط بهم الحوار لعقد اتفاقات حول خفض أعداد القوات ورفع بعض القيود عن المحتجين، والتصرف ضمن حدود معينة في مقابل التزامات محددة من جانب المحتجين للوصول بالموقف لحالة الاستقرار.
- إفهام المتظاهرين بأنه من غير المنطقي أن تتوقف الشرطة تمامًا عن استخدام القوة؛ لأن ذلك يخضع لحالات يلزمها القانون بحتمية استخدامها.
- العمل على دفع المحتجين لمسارات محددة والانتهاء بهم لموقع محدد لإبعادهم عن المواقع المهمة.

كما تضمن التكتيك التواصل الفعال مع المحتجين، ليس من خلال التواصل اللفظي فقط، ولكن من خلال رسائل رمزية أخرى، منها على سبيل المثال ما يلي:

- استخدام مكبرات الصوت.

(71) إبراهيم، تطبيقات علم النفس الاجتماعي في تعامل الشرطة مع الاحتجاجات، 74.

- توزيع نشرات صادرة عن الشرطة بتعليمات محددة بقصد توعية المحتجين بنصوص القانون أو شرح فكرة معينة أو تكذيب شائعة ... إلخ.

- استخدام صفارات الإنذار، وتكثيف الوجود الشرطي للقوات النظامية، والدفع بسيارات شرطة في موقع الحادث، وتنشيط مجموعات فض الشغب ومجموعات القبض.

هذه الرسائل الرمزية يمكن أن يكون لها دور إيجابي أثناء الحوار، ويمكن بث رسائل ضمنية من خلالها بجاهزية القوات للتقدم أو التراجع بحسب الأحوال، ويمكن تقليص القوات وتخفيف القيود عن المحتجين في مرحلة لاحقة، ويمكن النظر في تطوير هذه الرسائل بالزيادة أو النقصان بحسب طبيعة المشهد والملابسات المحيطة به[72].

وبالرغم من الانتقادات التي وجهت لهذا التكتيك في البداية، سواء من المحتجين الذين أخذوه على محمل الشبهة أم المكيدة أم عدم الثقة، أو من ضباط الشرطة السويديين الذين أبدوا تحفظهم على انخراط عناصر شرطية للحوار وسط الحشود دون تأمين، إلا أن التكتيك وجه انتباه المحتجين إلى نبذ العنف، ولمست الشرطة تراجع الفوضى واستشعرت أنها نجحت في اكتساب ثقة العامة وبدا سلوكها أكثر تقدمًا وتحضرًا[73].

وكانت إحدى النتائج المهمة التي أفرزها هذا التكتيك أن مجموعات الحوار المنوه عنها تطورت مع الوقت، وأصبحت منذ عام 2002 وحدة من وحدات العمليات الخاصة (SPT) داخل الهيكل التنظيمي للشرطة في السويد[74].

وقد كانت نقطة الانطلاق في عمل شرطة الحوار هي تحديد الأهداف والمبادئ الحاكمة للعمل، وكان من أهمها[75]:

- الاستعانة بشرطة الحوار في التظاهرات وفي المناسبات عالية الخطورة، سواء في مرحلة التخطيط بالنسبة للأحداث المعروفة مسبقًا، أم في المراحل التالية في التظاهرات غير المخطط لها وغير المصرح بها.
- لا يعتمد دور الشرطة في الطريقة الجديدة للتعامل مع الاحتجاجات على كسب المعركة ولكن يعتمد على محاولة تجنبها، ومن ثمّ فإن وسيلتها الأنسب في ذلك هي الحوار لنزع فتيل الأزمة والحد من مخاطرها.

(72) إبراهيم، تطبيقات علم النفس الاجتماعي في تعامل الشرطة مع الاحتجاجات، 75 وما بعدها.

(73) Stott, Clifford., Op.Cit, p.18.

(74) Holgersson, Stefan., Op.Cit, p.16.

(75) Ibid, pp.4042-.

- اعتماد استراتيجية الحوار في التعامل مع الاحتجاجات، وبالرغم من التشابه الكبير بين الحوار والتفاوض في بعض الجوانب، إلا أن الشرطة السويدية فضلت الحوار على التفاوض؛ إذ ينطوي التفاوض أحيانًا على استخدام بعض الحيل لخداع الطرف الآخر، وذلك عندما يتم اللجوء إليه في حالات الأزمات في أحداث فرديّة منعزلة، خاصة أنه عادة لا يتم التفاوض مع نفس الأفراد في مناسبات أخرى، أما عمل شرطة الحوار فينطوي على الاتصال المتكرر مع الأفراد أنفسهم في مناسبات مختلفة، وهو ما يتطلب بناء قدر من الثقة بينهما من خلال إقامة حوار حقيقي مبني على الاحترام المتبادل لتجنب تفاقم الأحداث.

وقد تم تقسيم مهام عمل شرطة الحوار إلى ثلاث مهام رئيسة: مهام قبل الحدث، ومهام أثناء الحدث، ومهام بعد الحدث، ومع ذلك قد يكون الأمر أكثر تعقيدًا في بعض الأحيان، فعمل شرطة الحوار في الظروف العادية يستلزم إنشاء حوار مستمر مع مجموعات تنظيم التظاهرات، وقد تترابط وتتداخل العديد من التظاهرات، فما يعد حوارًا بعد تظاهرة معينة قد يتحول إلى حوار قبل تظاهرة تالية، فضلاً عن ذلك يعد عمل شرطة الحوار جزءًا من عمل متكامل لأجهزة الشرطة المعنية بالتعامل مع التظاهرات[76].

أولاً: مهام شرطة الحوار قبل الحدث:

تهدف مهام شرطة الحوار إلى خلق بيئة من الاحترام المتبادل والتعاون لتجنب التصعيدات والاحتكاكات التي قد تنشأ عن عدم فهم الآراء والمواقف المتنوعة، وربما تمتد هذه المهام على مدار عدة أشهر[77]، وتنقسم مهام شرطة الحوار قبل الحدث إلى ما يلي:

1. التأثير على الحدث:

يوجد مهام لشرطة الحوار في الأحداث التي تم تقديم طلب للحصول على تصريح بها، ومهام أخرى في الأحداث التي لم يتم تقديم طلب للحصول على تصريح بها[78].

أ- الأحداث التي تم تقديم طلب للحصول على تصريح بها:

عادة ما يتضمن طلب التصريح، مكان بدء وانتهاء التظاهرة وخط سيرها، وتوقيت بدئها وانتهائها، وموضوعها والغرض منها ومطالبها، وأسماء الأفراد أو الجهة المنظمة لها.

ويكون الغرض الرئيسي من الحوار مع المنظمين في هذه الحالة هو الحصول على أكبر قدر ممكن من المعلومات عن التظاهرة، والتعاون معهم في تعديل أي من

(76) Holgersson, Stefan., Op.Cit, p.33.

(77) Waddington, David P., Op.Cit, p.32.

(78) Holgersson, Stefan., Op.Cit, pp.4248-.

البيانات السابقة إذا كان يترتب عليها بعض التداعيات الأمنية، مع التركيز خلال الحوار على فكرة التمكين من الحقوق، وتبادل الأدوار، والحفاظ على الدولة[79].

ب- الأحداث التي لم يتم تقديم طلب للحصول على تصريح بها:

تفترض هذه الحالة ورود معلومات للجهات الأمنية باعتزام بعض الأفراد أو الجهات تنظيم تظاهرة للتعبير عن رفضهم أو تأييدهم لموضوع معين.

ويكون الغرض الرئيس من الحوار مع المنظمين في هذه الحالة هو إقناعهم بتقديم طلب للحصول على تصريح، مع إخطارهم بأنهم سيكونون مسؤولين عن الحفاظ على النظام خلال التظاهرة، فضلاً عن ذلك السعي للحصول على معلومات عن مكان بدء وانتهاء التظاهرة وخط سيرها، وتوقيت بدئها وانتهائها، وموضوعها والغرض منها ومطالبها، وأسماء الأفراد أو الجهة المنظمة لها، والتعاون معهم في تعديل أي من البيانات السابقة إذا كان يترتب عليها بعض التداعيات الأمنية.

2. التعاون مع الشركاء الآخرين:

تقوم شرطة الحوار بتنظيم بعض الأنشطة مع شركاء خارجيين مثل الخدمات الاجتماعية وخدمات الطوارئ بهدف تقليل الأضرار التي تلحق بالممتلكات أو الإصابات التي تلحق بالأفراد، وكذا التعاون مع الأفراد المتطوعين المستعدين للمشاركة في نقل المعلومات للشرطة مع تأمين الاتصالات الخاصة بهم أو المستعدين لتنظيم أشياء مثل الطعام والشراب للحفاظ على القدرة على التحمل؛ إذ أكد بعض الباحثين على أهمية الأنشطة الجماعيّة ذات الطبيعة التطوعية في تقديم دعم فعال للديمقراطية[80].

3. المشاركة في التقديرات الأمنية:

نظرًا للخبرات المتراكمة لدى شرطة الحوار، لذا يمكنهم الإسهام بكمية كبيرة من المعلومات التي قد تكون مفيدة قبل بدء العمليات وعند بدايتها، على سبيل المثال: عدد المشاركين المتوقع حضورهم تظاهرة غير مصرح بها؛ إذ أثبتت التجارب العمليّة أن شرطة الحوار لها تحليلها الخاص لكل حالة على حدة[81].

(79) Waddington, David P., Op.Cit, p.37.

(80) Holgersson, Stefan., Op.Cit, p.46.

(81) Ibid, pp.4748-.

ثانيًا: مهام شرطة الحوار أثناء الحدث:

تعمل شرطة الحوار بالتعاون مع منظمي الحدث على ضبط النفس أثناء الاحتجاجات لتجنب حدوث أي اضطرابات أثناء الحدث[82].

1. التأثير على الحدث:

كما هو الحال في مهام شرطة الحوار قبل الحدث، من الطبيعي أن يكون الحوار مع منظمي الأحداث التي سبق تقديم طلب للتصريح بها أسهل من الحوار مع منظمي الأحداث التي لم يتم تقديم تصريح بها[83].

أ- الأحداث التي تم تقديم طلب للحصول على تصريح بها:

قد تتغير الأمور بسرعة أثناء الحدث، وقد تنشأ حاجة ملحة لإعادة تنظيم الحدث من حيث مكان بدايته أو نهايته أو خط سيره أو توقيت بدايته أو نهايته أو غيره، وقد تنتشر شائعات تؤدي إلى نشر جو معادٍ بين المتظاهرين أو بينهم وبين الشرطة.

لذا يمثل الحوار الدائم بين شرطة الحوار والمنظمين، من خلال الالتقاء المباشر بهم في بداية التظاهرة أو من خلال الاتصالات الخلوية، منطلقًا جوهريًا لتقليل المخاطر؛ إذ يمكن لضباط شرطة الحوار الاتصال بقادتهم للموافقة على تغيير خط سير التظاهرة أو تعديل موعدها، أو مدهم بالمعلومات الصحيحة في موضوع معين لمواجهة انتشار بعض الشائعات بين المتظاهرين.

ب- الأحداث التي لم يتم تقديم طلب للحصول على تصريح بها:

من الضروري وجود معلومات لدى الشرطة عن منظمي الحدث أو الأفراد المؤثرين فيه، وغالبًا ما يكونون معروفين لشرطة الحوار من مناسبات سابقة؛ لذا تكون الاتصالات السابقة معهم مهمة للغاية لإقامة حوار، ومن المهم التأكيد عليهم بحفظ النظام في المنطقة، وأن الشرطة سوف تتدخل في حالة عجزهم عن ذلك.

2. التعاون مع الشركاء الآخرين:

تتبلور مهمة شرطة الحوار في التعاون مع المتطوعين المستعدين للتعاون مع الشرطة من خلال الالتقاء بهم، وتنظيم وجودهم، وتحديد أدوارهم، وتنسيق عمليّة الاتصال بهم خلال التظاهرة، وتحديد آلية تلقي المعلومات منهم، بهدف الحفاظ على النظام العام.

(82) Waddington, David P., Op.Cit, pp.3840-.

(83) Holgersson, Stefan., Op.Cit, pp.5154-.

وفضلاً عن ذلك الاتصال بالأفراد المتأثرين بالحدث، مثل ملاك المحلات الموجودة في خط سير التظاهرة، وذلك بهدف تقليل الأضرار التي قد تلحق بالممتلكات أو الإصابات التي قد تلحق بالأفراد[84]، ويمكن تحقيق ذلك التواصل من خلال الرسائل النصية على أجهزة التليفون المحمول أو من خلال توزيع المنشورات[85].

3. المشاركة في التقديرات الأمنية:

تشارك شرطة الحوار باقي الأجهزة الأمنية في حفظ النظام العام خلال التظاهرة، وذلك بما لديها من معلومات وخبرات في هذا المجال، من خلال ما يلي:

أ- التنبيه بعواقب الأساليب الشرطية:

تتضمن هذه المهمة لفت انتباه صانعي القرار إلى العواقب المحتملة لإجراء وشيك أو عمل ما من أعمال الشرطة على سلوك الحشود على المدى القصير والبعيد، والتأكد من أن الطرف المقابل لا يشعر بالخداع أو الخيانة وهو أمر ذو أهمية حاسمة للقدرة على إقامة حوار مثمر في المستقبل.

ويشار في هذا الصدد إلى أن الموقف الذي تتخذه شرطة الحوار في حشد من الناس يوفر عادة فرصة جيدة لرؤية سلوك الشرطة من وجهة نظر المتظاهرين؛ لذا فإن القدرة على لفت انتباه صانعي القرار إلى تغيير أساليب الشرطة التي ينظر إليها على أنها غير وديَّة من وجهة نظر المتظاهرين هي عامل مهم في تجنب تصعيد الموقف، وبذلك يجد الأفراد الذين لديهم الرغبة في مواجهة الشرطة صعوبة أكبر في تحقيق هدفهم[86].

ب- التنبيه بالحالة العامة للحشد:

توصف الحالة العامة للحشد وفقًا للون، فعندما توصف بأنها خضراء فذلك يعني أنها هادئة، وعندما توصف بأنها صفراء فذلك يعني أنها غير واضحة، وعندما توصف بأنها حمراء فذلك يعني أن الوضع خطير.

وقد ينظر البعض إلى الحالة على أنها "حمراء" أي خطيرة في جزء من تظاهرة، في حين ينظر إليها في جزء آخر على أنها "خضراء" أي هادئة، ويرجع ذلك إلى تنوع المجموعات التي يتكون منها الحشد واختلاف نياتها وتوجهاتها.

(84) Holgersson, Stefan., Op.Cit, pp.5457-.

(85) Waddington, David P., Op.Cit, p.35.

(86) Holgersson, Stefan., Op.Cit, pp.5761-.

ونظرًا للخبرة الواسعة التي يكتسبها ضباط شرطة الحوار من وجودهم في أحداث سابقة، ومن ملاحظاتهم لسلوك الحشود لفترة أطول، فإنه يسهل عليهم فهم وتفسير سلوك الحشد ككل بمجموعاته ومكوناته كافة، ومن ثمّ التنبيه بالحالة العامة للحشد تنبيهًا دقيقًا[87].

ج- التنبيه بالتطورات المحتملة:

تتضمن هذه المهمة الجهود المستمرة للتنبؤ بالتطورات المحتملة وإبلاغ القادة بها، ويتطلب ذلك القدرة على إدراك الواقع من خلال تواجدهم داخل الحدث، وتحليل الظروف الحرجة في المواقف المختلفة، والتنبؤ بالمسار المحتمل للأحداث[88].

4. العمل على خفض التصعيد:

أظهرت الأبحاث العلميّة والتجارب العمليّة أن مستوى العداء ضد الشرطة يكون أقل بكثير إذا كان ضباط الشرطة يتعاملون مع أفراد الحشد بطريقة ودية ومنفتحة، عما هو عليه عند اعتماد استراتيجية تتبنى الحفاظ على مسافة آمنة، ومعاملة الحشد بحذر، وتجنب التفاعل غير الرسمي معهم.

كما أكدت أن وجود ضباط شرطة الحوار بين الحشد له تأثير معتدل على مجرى الأحداث؛ إذ يقلل من تأثير عدم الكشف عن الهوية[89] بين النشطاء، فضلاً عن أن الاتصالات السابقة والثقة مع بعض الأفراد يمكن أن يجعل الحوار أسهل.

كما أن وجود ضباط شرطة الحوار بدون أسلحة يمكن أن يساعد في توضيح أن شرطة الحوار موجودة لمساعدة هؤلاء الأفراد على السماح لهم بالتظاهر وعدم استخدام الوسائل القسرية ضدهم[90].

5. التعامل مع المواقف الطارئة:

قد تنشأ بعض المواقف الطارئة خلال الحدث، مثل إصابة أحد أفراد التظاهرة، أو تعرضه لوعكة صحية، أو نشوب حريق بأحد الأماكن.

(87) Ibid, pp.6163-.

(88) Holgersson, Stefan., Op.Cit, pp.6365-.

(89) قامت بعض الأبحاث النفسية بدراسة تأثير عدم الكشف عن الهوية على سلوك الحشود؛ حيث انتهت إلى أن عدم الكشف عن الهوية قد يدفع أعضاء المجموعة للانخراط في سلوكيات غير اجتماعية وربما معادية للمجتمع، ومن المرجح أن تحدث هذه السلوكيات في المجموعات الكبيرة وفي الظلام

راجع: سعد الدين، أيمن. إدارة الحشود في العمل الأمني (القاهرة، بدون دار نشر، الطبعة الثالثة، 2022)، 49 - 50.

(90) Holgersson, Stefan., Op.Cit, pp.6670-.

ويؤدي ضباط شرطة الحوار دورًا مهمًا في هذه الحالة؛ حيث يعملون على تقديم المساعدة العاجلة من خلال الاتصال بالخدمات الاجتماعية وخدمات الطوارئ[91]، وتدرك الشرطة أن هذه الأعمال تلزم المنظمين ضمنيًا بالاحترام والتعاون لتجنب التصعيدات والاحتكاكات، فضلاً عن تولي موقع المسؤولية عن المشكلات المحتملة[92].

ثالثًا: مهام شرطة الحوار بعد الحدث:

لا تنتهي مهمة شرطة الحوار بانتهاء الحدث، ولكنها تعمل دائمًا على الاستفادة من المواقف والأحداث السابقة بهدف الاستعداد للأحداث التالية، من خلال ما يلي:

1. **التواصل مع الجهات الخارجية:**

تعمل شرطة الحوار على عقد اجتماعات تنسيقية مع منظمي التظاهرة ومع الشركاء الخارجيين؛ إذ يعزز ذلك الثقة والاحترام المتبادل بين الطرفين، فضلاً عن أنه يتيح الحصول على تعليقات قيمة حول عمليات الشرطة خلال الحدث.

2. **التقييم:**

تعمل شرطة الحوار على استخلاص المعلومات المفيدة مثل آراء المشاركين في الحدث والتي تتضمن الإيجابيات والسلبيات التي واجهت الشرطة؛ حتى يتم تعزيز الإيجابيات والعمل على تلافي السلبيات في الأحداث المقبلة[93].

المطلب الثاني: التجربة الكندية

تناولت إحدى الدراسات العلميّة[94] مقارنة بين أسلوب شرطة مكافحة الشغب الكندية خلال حدثين مهمين: الأول قمة الأميركتين التي عُقدت في مدينة كيبيك عام 2001، والآخر مؤتمر مجموعة الثماني الذي عُقد في مدينة كاناناسكيز عام 2002، وكيف تغير الأسلوب الشرطي من الأسلوب التقليدي الذي يعتمد على استخدام القوة الخشنة في التعامل مع المتظاهرين، إلى الأسلوب المستحدث الذي يعتمد على بناء الثقة بين الشرطة والمتظاهرين ويتضمن بعض الأدوات، مثل جمع المعلومات، والمراقبة، وإجراء الحوار، والتفاوض.

(91) Ibid, pp.7072-.

(92) Waddington, David P., Op.Cit, p.33.

(93) Holgersson, Stefan., Op.Cit, pp.7375-.

(94) "King, Mike., Op.Cit.

أولًا – الحدث الأول: قمة الأميركتين، مدينة كيبيك، 20 – 22 أبريل 2001:

خلال انعقاد القمة الأولى لدول الأميركتين (34 رئيس دولة من دول أمريكا الشمالية والجنوبية) في سانتياجو عام 1998، تم الإعلان عن موعد ومكان عقد القمة الثانية في مدينة كيبيك الكندية خلال شهر أبريل 2001، كما تم الإعلان عن جدول أعمال هذه القمة والذي يتناول الموضوع الشائك والجدلي الخاص بإنشاء سوق حرة مشتركة بين دول الأميركتين (FTAA)[95]، وقد وفر هذا الإعلان ثلاثة أعوام من التحضير والاستعداد لكل من الشرطة الكندية والمعارضين أيضًا؛ إذ إن حركة مناهضة العولمة (Anti-Globalization Movement) كانت ضد بنود هذه الاتفاقية وترى أنها سوف تزيد الأغنياء غنىً وتزيد الفقراء فقرًا.

وقد بدا واضحًا من البداية أن الهدف الرئيس للشرطة هو حماية الشخصيات المهمة الموجودة بالقمة وأن تسير فعاليات القمة دون مقاطعة، ولتحقيق هذه الغاية وظفت الشرطة عقلية "الحِصن"؛ تم التجهيز لأكبر عمليّة شرطية في تاريخ كندا، وقد رصدت الحكومة الكندية مبلغ 100 مليون دولار كندي لتأمين الحدث، وشارك في تأمينه أكثر من 6000 ضابط شرطة، كما تم وضع كردون أمني بمسافة 6.1 كيلو متر، بالإضافة إلى إنشاء سور حديدي عملاق بارتفاع 3 أمتار وبطول 3.8 كيلو متر تم اختباره ليتحمل 20 ألف رطل من الضغط.

كما تم تعيين أربع قوات شرطية لتأمين الحدث، وتحديد دور لكل قوة في وجود لجنة مشتركة للتنسيق بين القوات، الأولى هي "شرطة كيبيك" المسؤولة عن التدخل في حالات الطوارئ المدنية والتنسيق مع الهيئات المحلية، والأخرى هي "بلدية كيبيك" المسؤولة عن البحث الجنائي وعمليات القبض والتفتيش وحماية مداخل ومخارج السور للمواطنين والمشاركين في القمة، والثالثة هي "الشرطة الملكية" والتي تحملت المسؤولية الأولى عن التخطيط العملياتي والتنسيق بين القوات، والرابعة هي "الدعم العسكري" وتحملت مسؤولية تأمين الموقع وحماية الشخصيات المهمة والعلاقات العامة وتقييم المخاطر والتهديدات.

وقد تم الاتفاق بين "الشرطة الملكية" وبين قادة المتظاهرين على نقاط رئيسية أهمها ألا يقتربوا من محيط السور، وأن يلتزموا بحدود الدوائر الأمنية؛ إذ تم تحديد ثلاث دوائر لأنشطة المتظاهرين ولتعامل الشرطة معهم: الدائرة الأولى "الخضراء" (للمتظاهرين بالشكل الاحتفالي)، والدائرة الثانية "الصفراء" (تشمل المحتجين في نطاق تحت السيطرة)، والدائرة الثالثة "الحمراء" (تشمل المشاغبين المرتكبين لأعمال جنائية).

(95) "Free Trade Area of the Americans".

في بداية الحدث التزم الحشد بالاتفاق بعدم الاقتراب من محيط السور، وتم تأمينهم بالأمن العادي (ذوي القبعات الناعمة[96])، إلا أنهم لم يلبثوا أن كسروا السور في اليوم الأول للقمة (20 أبريل)، وفي اليوم الثاني استخدم المتظاهرون طوال ثلاث ساعات 12 عبوة مولوتوف وقذفوها على تشكيل للشرطة الملكية (مكون من 32 فردًا من مكافحة الشغب)، وقد بدت قوات مكافحة الشغب في البداية تدافع عن السور فقط، ولكن بعد خرقه تم تعزيز القوات بقوات ملكية إضافية من مدن مجاورة، مثل نوفاسكوتيا، ونيوبرونزويك، وأونتاريو، ومن اليوم الثاني كانت هناك توغلات خارج المحيط الأمني.

وقد شمل تسليح الشرطة بالإضافة إلى وحدات القناصة، مدافع المياه، والصواعق الكهربية، ورشاشات مسحوق الفلفل، والطلقات البلاستيكية عيار 37 ملم، وتم إطلاق 5148 قنبلة غاز، و903 طلقات بلاستيكية، ورغم أن الطلقات الدافعة كانت غير مصرح باستخدامها إلا أن بعض القوات استخدمتها تحت وطأة سخونة الأحداث، كما تم إلقاء القبض على 463 شخصًا.

وقد وصف شاهد عيان المشهد بأنه كان خليطًا من الاحتفال والفوضى، وسط سحابة من دخان الغاز؛ إذ حاول المحتجون اختراق السور وهدمه مع قذف قوات الشرطة بالطوب والحجارة، وقامت قوات الشرطة بالتعامل معهم بعنف، الأمر الذي أسفر عن سقوط العديد من الإصابات والوفيات، وقد ذكر أحد المتظاهرين أنه لم يكن لهم صوت مسموع لدى الوفود المشاركة في القمة، ولكن في الواقع "مجرد كسر السور كان بمثابة نصر رمزي لهم"، وعلى هذا الأساس تُعد العمليّة الشرطية في المجمل ناجحة، ولكن تبقى مسألة الإفراط في استخدام قنابل الغاز المسيل للدموع، ومسألة وقفة قوات الشرطة موقف التحدي مع المتظاهرين، ومسألة السور المرتفع الذي يعزل موقع الحدث، علامات استفهام على الأداء الشرطي خلال هذه القمة[97].

ثانيًا - الحدث الثاني: قمة مجموعة الثماني، كاناناسكيز 26-27 يونيو 2002:

كان الوقت المتاح للتخطيط لعمليّة تأمين هذه القمة قصيرًا جدًا بالمقارنة بقمة كيبيك؛ إذ كان مقررًا عقد القمة في العاصمة أوتاوا، إلا أنه بعدما حدث في قمة مجموعة الثماني في جنوا في سبتمبر 2001، أعلن رئيس الوزراء الكندي (جون شيرتيان) أن قمة مجموعة الثماني سوف تعقد في يونيو 2002 في قرية جبلية نائية في مقاطعة كاناناسكيز، ألبرتا،

(96) ثمة تفرقة في النظام الغربي بين القبعات الناعمة "soft hats" التي ترتديها الشرطة العادية في الشارع، وتوحي بالتعاون والحماية والالتحام مع الجمهور، وبين القبعات الصلبة "hard hats"، أي الخوذات التي ترتديها قوات فض الشغب مع الدرع والعصا، وتوحي دومًا بتوتر الأجواء واحتمالية التدخل وحدوث أعمال عنف

(97) سعد الدين، إدارة الحشود في العمل الأمني، 110 112-.

90 كم غرب كالجاري، وقد كان هذا القرار بتغيير موقع عقد القمة مفاجئًا للمعارضين إلا أنه فتح بابًا لخلق أماكن أخرى رمزية للاحتجاج وليس بالضرورة موقع الحدث نفسه، ونذكر منها مكانين فقط هما كالجاري (أقرب مدينة لموقع القمة)، وأوتاوا (العاصمة)، بالإضافة إلى الترتيبات الأمنية في كاناناسكيز نفسها[98].

1. في كاناناسكيز وكالجاري:

لقد جعل الموقع الجغرافي للقمة مهمة الشرطة أكثر تعقيدًا من قمة كيبيك، ورغم ذلك كانت "الشرطة الملكية" تتقلد الأدوار نفسها بخصوص تأمين الشخصيات المهمة بصفتها الشرطة الفيدرالية، كما استمرت الشرطة المحلية في مدينة كالجاري في أداء مهامها الأمنية داخل المدينة بما يشمل قوات مكافحة الشغب، بينما لعبت وزارة الدفاع دور "الدعم الأمني" في المحيط الأمني لمدينة كاناناسكيز فيما يتعلق بالدعم اللوجيستي والدعم الجوي، كما ضمت العمليّة الشرطية قوات إضافية من جهات مختلفة، مثل الشرطة المحلية لإدمونتون، وساسكاتون، وفانكوفير، وأونتاريو، وكما حدث في كيبيك كانت مهمة الشرطة الأساسية هي استمرار القمة وعدم مقاطعتها، وكان ثمة هدف آخر للقوات وهو التأمين ضد الهجمات الإرهابية[99]، في ظل تلك المعطيات حصلت هذه العمليّة على لقب أكبر عمليّة شرطية في تاريخ كندا المعاصر (أكبر من عمليّة كيبيك).

وكما كان الوضع في كيبيك، تم تحديد دوائر لفصل أنشطة المتظاهرين وتعامل القوات، وقد كانت هناك ثلاث دوائر ملونة: المنطقة الحمراء، لنصف قُطر 2 كم حول موقف القمة ويشمل فندق إقامة المشاركين، وقد لعبت القوات المسلحة دور الداعم للشرطة في الدعم اللوجيستي والتغطية الجوية، وتولت الشرطة الملكية مهمة تأمين المباني ورئيس الوزراء والشخصيات المهمة، والمنطقة الزرقاء، لنصف قطر 6.5 كم وكانت فيها دوريات تقودها القوات المسلحة، والمنطقة الصفراء، لنصف قطر 20 كم وتحملت مسؤوليتها الشرطة الملكية بصحبة الدعم العسكري، كما تم غلق عدد من الطرق بين كاناناسكيز وكالجاري، وقد ذكرت الصحف أن رئيس الوزراء الكندي كان يداعب الصحفيين الإيطاليين بقوله إن موقع القمة كان محميًا من الخلف بالجبال ومن الأمام بالنهر ومن الجنوب بقرية هندية ومن الشمال بخمسمائة دب شرس، كما تم تحديد مسافة 150 كم منطقة حظر طيران فوق موقع القمة.

(98) المرجع السابق، 112.

(99) وقت انعقاد القمة كان بعد أحداث 11 سبتمبر 2001 بأقل من سنة، وكان الهاجس الإرهابي ما زال يخيم على جميع العمليات

وبخلاف قمة كيبيك التي اتسمت بالإجراءات الأمنية المشددة والقمعية والإقصائية، كانت عمليّة كاناناسكيز أهدأ نوعًا ما، وكانت قوات الشرطة ترتدي القبعات الناعمة مع الاعتماد الكلي على الاستخبارات والمراقبة والتواصل مع المتظاهرين، أما قوات فض الشغب فكانت على كامل استعدادها ولكن بعيدًا عن الأنظار؛ حيث تم دعم العمليّة بعدد 12 مركبة مدرعة من القوات المسلحة، ومدفعين للمياه (لم يُستخدموا)، وذخيرة فض شغب وغاز مسيل للدموع بالإضافة إلى وحدة خيالة ووحدة كلاب حراسة، وكان الخط الأمامي في مواجهة المتظاهرين وحدة دراجات هوائية منظمة في فصائل، وتستخدم لجمع المعلومات من الميدان ومدربين على العمليات التكتيكية باستخدام الدراجات.

وفي الميدان، لم يتخط عدد المتظاهرين 2500 فرد، ولم يتم استدعاء قوات فض الشغب إلا في واقعة واحدة في اليوم الأول للقمة؛ إذ قام عدد 30 من المتظاهرين بالاعتصام في محل مأكولات بوسط المدينة، أما باقي الاحتجاجات فكانت سلمية واحتفالية، كما حدث في اليوم الأول مسيرة احتجاجية من 1000 شخص على شكل أفعى "Snake March"، أما في دائرة محيط كاناناسكيز؛ حيث تُقام القمة فكان الوضع هادئًا، كما توجه في اليوم الأول 200 شخص تقريبًا في موكب إلى موقع المؤتمر ولكن تم إيقافهم لدى أول نقطة تفتيش، كما وصلت حافلة تحمل 30 محتجًا إلى نقطة التفتيش الثالثة، وكانت تحمل ملصقات وعدد 400 من الخطابات والمنشورات الاحتجاجية وتم تسليمها لشرطة نقطة التفتيش لتوصيلها لقمة الثمانية، وتم القبض على محتج واحد فقط، وفي اليوم الثاني حاول 50 محتجًا أن يخرقوا الكردون الأمني وتم إلقاء القبض على شخص واحد[100].

2. في أوتاوا:

كان الهدف الرئيسي للشرطة الملكية في أوتاوا هو تأمين البرلمان والمنشآت الفيدرالية المهمة والسفارات، بالإضافة إلى ضمان سلامة المتظاهرين وتنظيمهم أثناء انعقاد قمة الثماني، وحماية الأرواح والممتلكات، وصون حقوق الأفراد وسلامتهم، ولتحقيق هذه الغاية اعتمدت الخطة العملياتية لجهاز الشرطة بمدينة أوتاوا على أنه "لن يتم الاستعانة بقوات فض الشغب، إلا إذا ارتأى قائد العمليّة ضرورة الاستعانة بهم في الحالات التي تقتضيها الضرورة وحسب سير الأحداث، وستظل شرطة أوتاوا المحلية بالقبعات الناعمة". كما أن السياسة الجديدة فرضت عدم إنشاء أية أسوار حديدية مرة أخرى.

وعلى غرار الأحداث السابقة، اشترك عدد من القوات والأجهزة الشرطية في العمليّة، منها القوات الفيدرالية، والشرطة التابعة للمقاطعة، وشرطة البلدية أيضًا لسد احتياجات الخدمات الأمنية المطلوبة.

(100) سعد الدين، إدارة الحشود في العمل الأمني، 113- 114 .

وقد ارتكزت سياسة "القبعات الناعمة" التي انتهجتها الشرطة الكندية في أوتاوا على تشكيل "فريق الشرطة المجتمعية"، الذي كان هدفه التواصل والوساطة مع جميع الأطراف خاصة ممثلي المحتجين في مراحل ما قبل الحدث وأثناءه وبعده، بجانب جمع المعلومات والأدلة وتحقيق المراقبة الاستباقية لدى مواقع التظاهرات، وإعداد الخطط البديلة لتدخل فرق فض الشغب الموجودة بعيدًا عن الأنظار ولكن على أهبة الاستعداد، وتحرك فصيلة الدراجات الهوائية التي من شأنها تحقيق الاستخبارات لحظة بلحظة من موقع الحدث بالإضافة إلى توجيه الحشود بِرِفق.

وقبل الحدث بأربعة أشهر تم تشكيل مجموعة مشتركة لجمع المعلومات مُشكّلة من ممثلين لجهاز الشرطة الكندي ولأجهزة استخبارات أمريكية، وبدؤوا برنامجًا نشطًا لجمع المعلومات عن النشطاء وتخطيطهم وأنشطتهم، ومن النتائج التي توصلت لها المجموعة تمكنوا من عمل التالي

- تحديد هويات النشطاء وتتبع حركتهم.
- تحديد الحافلات الناقلة للمحتجين إلى أوتاوا قبل مغادرة مدينة التحرك، وتعقبهم طوال الطريق من طائرة هليكوبتر تابعة للشرطة الكندية.
- ترقب وصول الحافلات في أوتاوا، وبمجرد وصولهم تم تصوير جميع الركاب.

كما تم عقد منتديات قبل بدء القمة مع المتظاهرين لمناقشة مطالبهم وحضر تلك اللقاءات فريق الشرطة المجتمعية (وبه ممثلون من كل الوحدات الشرطية المشاركة) مع ممثلي وقادة المحتجين (من حركة مناهضة العولمة).

ويرجع التغيير الواضح في السياسات والممارسات الذي جرى اتباعه في أحداث أوتاوا وما تبعه من هدوء في الحالة الأمنية وعدم نشوب صراعات بين قوات الشرطة والمتظاهرين إلى أربعة أسباب

- الطقس الممطر طوال يومي عقد القمة؛ ما عطل الكثيرين من الانخراط في الاحتجاجات.

- التخطيط المُسبق وجمع الاستخبارات والتعاون بين قوات الشرطة المختلفة ونشر المعلومات بينهم، واتباع سياسة "عدم التسامح مطلقًا" في التعامل مع المخالفين، وذلك من خلال توضيح الخط المرسوم لتحديد منطقة نشاط المحتجين وأي اختراق للخط أو انتهاك للقانون يتم الاستجابة له بالقبض الانتقائي الفوري، وأهم أداة ساعدت على تحقيق ذلك هي استخدام كاميرات المراقبة الفعالة لجمع الأدلة، كما أنها أدت دورًا كبيرًا كرادع للمتظاهرين والنشطاء المعروفين لعلمهم أن كل تصرفاتهم مرصودة بالكاميرات.

- الحضور الكبير لرجال الشرطة من ذوي القبعات الناعمة وزِي الشرطة التقليدي، وانزواء قوات فض الشغب أصحاب الخوذات بعيدًا عن المشهد.
- إصدار الولايات المتحدة قوانين مكافحة الإرهاب في أعقاب أزمة 11 سبتمبر؛ إذ كان لها تأثير سلبي على المحتجين وسببت لهم قلقًا من أن يتم وصمهم بالإرهابيين.

وقد وجّه رئيس جمعية الحريات المدنية إلى رئيس الشرطة في أوتاوا خطابًا أعرب فيه عن تقديره للجهود التي بذلتها الشرطة لحماية المعارضة المشروعة خلال تأمين احتجاجات مجموعة الثماني، وذكر الخطاب "لقد كان النهج الذي نهجته قواتكم صحيحًا، وذلك من خلال إبعاد قوات التعامل مع الشغب المحتمل عن المشهد (الكلاب- قوات فض الشغب- الأسلحة) وبذلك تحاشيتم المظهر "المهدِّد والمستفِز" للمتظاهرين، فقد كان تعامل الشرطة مع مراحل قبل الحدث وأثناءه وبعده أهلاً للثقة والتقدير لما فيه من الحرص على سلامة المتظاهرين وتطبيق القانون على المخالفين".

المطلب الثالث : التجربة البريطانية

تعرضت شرطة العاصمة الإنجليزية سكوتلاند يارد[101] لانتقادات حادة في أعقاب أعمالها المثيرة للجدل خلال الاحتجاجات التي تزامنت مع انعقاد قمة مجموعة العشرين[102] في لندن عام 2009 نظرًا لاستخدامها تكتيكات مفرطة في القوة أدت إلى إصابة واعتقال المئات من المتظاهرين، فضلاً عن موت أحد المارة الأبرياء متأثرًا بجروح أصيب بها أثناء اعتداء غير مبرر من أحد ضباط الشرطة[103].

وتحت ضغط سياسي وإعلامي مكثف، تم إجراء تحقيق من قبل رابطة مفتشي الشرطة التابعة للمملكة المتحدة (HMCIC)[104] لتقييم أعمال الشرطة أثناء الاحتجاجات، وكان

(101) هي قوة شرطة إقليمية مسؤولة عن حفظ الأمن في جميع أنحاء العاصمة الإنجليزية لندن باستثناء الجزء الداخلي.

(102) مجموعة العشرين هي منتدى للتعاون الاقتصادي والمالي بين بعض الدول وجهات ومنظمات دولية تلعب دوراً محوريا في الاقتصاد والتجارة في العالم وتجتمع سنويًا في إحدى الدول الأعضاء فيها، وأعضاؤها هي (الأرجنتين، أستراليا، البرازيل، كندا، الصين، الاتحاد الأوروبي، فرنسا، ألمانيا، الهند، إندونيسيا، إيطاليا، اليابان، المكسيك، روسيا، المملكة العربيّة السعودية، جنوب أفريقيا، كوريا الجنوبية، تركيا، المملكة المتحدة، الولايات المتحدة الأمريكية)، ويحضر اجتماعاتها بعض المنظمات والهيئات الدولية مثل (صندوق النقد الدولي، البنك الدولي، منظمة التجارة الدولية، مجلس الاستقرار المالي، منظمة التنمية والتعاون الاقتصادي، منظمة العمل الدولية، منظمة الأمم المتحدة)، كما يحق لرؤساء الدول المشاركة في القمة دعوة زعماء من خارج المجموعة

(103) Waddington, David P., Op.Cit, p.31.

(104) Her Majesty's Chief Inspector of Constabulary.

لتقاريرها تأثيرات بعيدة المدى باعتبارها تجمع كبار ضباط الشرطة بالمملكة؛ إذ أشارت إلى التغير الذي حدث في عالم الاحتجاج نتيجة التمتع بالديمقراطية بشكل أكبر، وما يتطلبه ذلك من تغير في الإدارة والممارسات، وأكدت أنه ينبغي استخدام المشاركة والحوار مع المتظاهرين كلما أمكن ذلك، كما اعترفت بالتحديات التي تواجه تطوير نهج يرتكز على الاتصال بين الشرطة والمتظاهرين، وأشارت إلى أهمية الاستفادة من نماذج الاتصال التي طورتها دائرة الشرطة في أيرلندا الشمالية (يشار إليها باسم نهج "لا مفاجآت") و"شرطة الحوار" التابعة لقسم شرطة ستوكهولم بدولة السويد[105].

ولم تغفل التقارير الإشارة إلى الدراسات النظرية الحديثة في مجال علم النفس الاجتماعي، وخاصة: نموذج الهوية الاجتماعية المفصل لسلوك الحشود (ESIM)، والذي يقدم أساسًا نظريًا لفهم سيكولوجية الحشود، ويؤكد على الحاجة إلى العلم بالظروف التي أدت إلى وجود الحشد والنيات المشروعة لأفراده، وأهمية اتباع نهج شرطي يتجنب الاستخدام غير المتمايز للقوة؛ إذ لا ينبغي افتراض أن الحشد بأكمله يشكل تهديدًا للنظام العام، كما أنه لا ينبغي إهمال التواصل مع الحشد؛ إذ إن التواصل معه ضروري للحفاظ على النظام؛ لأن الناس داخل الحشد "يمارسون الشرطة الذاتية" أو "ينظمون أنفسهم بأنفسهم".

كما أشارت الدراسات النظرية إلى المكونات الأساسية الخمسة لضبط الحوار وهي: التفاوض، والوساطة، والبدء "اقتراح الحلول الممكنة للمشاكل"، والتواصل، والاستشعار "التقييم المستمر للتهديد الذي يتعرض له النظام العام أثناء حدث جماهيري"، وأكدت على أن يعمل ضباط الحوار قبل وبعد الأحداث الجماهيرية لإقامة علاقات طويلة الأمد قائمة على الثقة والاحترام المتبادل مع المتظاهرين، علمًا بأن القدرة على الاستفادة من هذه العلاقات هي التي تحكم فعالية نهج الحوار، ومع ذلك، فمن المسلم به أن الحفاظ على مثل هذه العلاقات قد يكون أمرًا صعبًا، فمن ناحية يجب التأكيد على شفافية الشرطة في تعاملها مع مجموعات الاحتجاج، ومن ناحية أخرى يجب مراعاة عدم نبذ مسؤولي الحوار من قبل زملائهم "ألا ينظر إليهم على أنهم خونة"، أو من قبل المتظاهرين "ألا ينظر إليهم على أنهم مخادعين وجامعي معلومات استخباراتية".

وفي ضوء هذه التحديات، اكتشف مسؤولو الشرطة بالمملكة المتحدة أن التحرك نحو الحوار أمر جيد من الناحية النظرية ولكنه صعب من الناحية العمليّة، ومن ثم فإنه يوجد حاجة ملحة لأبحاث عمليّة ترتكز إلى أسس تجريبية، وقد وجدت الشرطة في مؤتمر الربيع

(105) Gorringe, Hugo, Clifford Stott, and Michael Rosie. "Dialogue police, decision making, and the management of public order during protest crowd events." Journal of investigative psychology and offender profiling 9.2 (2012), p.112.

لعام 2011 الذي يستضيفه الحزب الليبرالي الديمقراطي في مدينة شيفيلد الإنجليزية فرصة جيدة لدراسة تجريبية لتطوير تكتيك شرطي يعتمد على المفاهيم التي طرحها نموذج الهوية الاجتماعية المفصل لسلوك الحشود (ESIM)[106].

وقد انعقد المؤتمر على مدار ثلاثة أيام: من الجمعة 11 إلى الأحد 13 مارس 2011، وكان يبدو من البداية بأنه سوف يصبح مجالاً خصبًا للمعارضة والاحتجاج، نظرًا لدعم الحزب لتقليص القطاع العام فضلاً عن تراجعه عن تعهده بمعارضة الزيادات في الرسوم الدراسية للطلاب، وبالنظر إلى التاريخ الحديث للعنف في الاحتجاجات الطلابية السابقة، كان من المتوقع أن تسير الأحداث في السياق ذاته خلال هذا المؤتمر.

وقد كانت للشرطة مخاوف كبيرة من احتمال حدوث تدافع وسحق أثناء الاحتجاج؛ لأن المنطقة المخصصة للاحتجاج كانت محدودة المساحة نسبيًا، ولا يوجد بها سوى محاور ضيقة للخروج، وكان الحل الذي توصلت إليه هو تصميم سياج حديدي لتطويق مكان المؤتمر وموقع الاحتجاج بأكمله حيث كان بارتفاع الخصر فقط في بعض الأماكن، وذلك للسماح بخطوط سير واضحة من الموقع إلى مكان الاحتجاج، مع السماح في الوقت نفسه بتوفير وسائل التأمين الكافية لتجنب نشر وحدات النظام العام (ذوي السترات الصفراء) في الحشد لمنع التوغل في مكان انعقاد المؤتمر.

وعلى الرغم من الاستعدادات الأمنية رفيعة المستوى، إلا أن الشرطة كانت مصممة على تطوير تكتيك شرطي يعتمد على الحوار. ومع ذلك، وخلال التفاعلات الأولى مع منظمي الاحتجاج، لاحظت الشرطة كيف أن البعض "أعادوا صياغة" فهمهم لـ "الشرطة" بالإشارة إلى المظاهرات الطلابية الأخيرة في لندن التي اتسمت بالعنف ضد المتظاهرين، كما انعكس ذلك من خلال وسائل الإعلام وتجارب الطلاب المحليين.

وقد قامت الشرطة بتحديد الاستراتيجية والنهج التكتيكي ودور "فريق اتصال الاحتجاج" (PLT)[107] الذي تم إنشاؤه خصيصًا من عدد 12 ضابطاً وضابطة، والتأكد من أنهم على دراية تامة بمسؤولياتهم وأن لديهم دورًا محددًا بشكل صحيح، وبمجرد اختيار فريق القيادة تم عقد اجتماع تخطيطي يضم القادة الرئيسيين لتحديد أولوياتهم الاستراتيجية، وتم الاتفاق على أن يكون فريق اتصال الاحتجاج هو المعني بتعزيز "التواصل الفعال" و"العلاقات" بين الشرطة والمحتجين. بالإضافة إلى ذلك، القيام بدور "التقييم المستمر للحالة الأمنية" و"نقل صورة واضحة عن المخاطر لتجنب الاستخدام غير المتمايز للقوة"، ومن ثمّ "تعظيم تصورات الحشد" حول شرعية عمل الشرطة، ولعل الأكثر أهمية هو كيفية ربط فريق

(106) Ibid, p.113.

(107) protest liaison team.

اتصال الاحتجاج بهيكل القيادة خلال الحدث؛ حيث تم إبقاء فريق اتصال الاحتجاج منفصلاً عن القنوات الراديوية للقيادة حتى لا يكون على علم بعمليات انتشار الشرطة الأخرى[108].

وقد بدأ فريق اتصال الاحتجاج في تطوير العلاقات مع منظمي الاحتجاج وتمكن بسرعة كبيرة من فهم أهدافهم ونياتهم، وقد أعطت هذه المعلومات قادة الشرطة الثقة في دقة وسلامة التخطيط للأحداث والتي بدأت في وقت متأخر من بعد ظهر يوم الجمعة باقتراح "الإضراب عن الدراسة" واحتجاجات من قبل مجموعات سياسية أخرى. وبحلول الساعة الرابعة صباحًا، كان هناك حوالي 100 متظاهر في وسط المدينة، وتحدث فريق اتصال الاحتجاج الذي كان يرتدي زيًا عاديًا مع علامات زرقاء مصممة خصيصًا تحمل علامة "ضابط الاتصال" مع المتظاهرين، وأشرك فريق اتصال الاحتجاج الناس من خلال توزيع منشورات إعلامية تشرح الأهداف الأساسية لعمليات الشرطة ودورهم المحدد في المساعدة على تسهيل الاحتجاجات، وضمان الحفاظ على حقوق الإنسان، وإبلاغ المتظاهرين بأسباب أي إجراءات تقوم بها الشرطة.

وقد قوبل فريق اتصال الاحتجاج ببعض الشكوك من قبل المتظاهرين، ومنهم من اعتبرهم "جواسيس للشرطة"، وعلى الرغم من الجهود المتعددة لفريق الاتصال إلا أن الجماعات الأكثر تطرفًا قاومت محاولات التواصل معهم، ولكن خلال الاحتجاج الأول قامت شخصية بارزة من إحدى هذه المجموعات بإعداد طاولة لتوزيع المنشورات؛ ما مكن فريق اتصال الاحتجاج من إقامة علاقات جيدة معهم.

وجاء الاختراق الثاني عندما تحرك المتظاهرون، الذين يبلغ عددهم عدة مئات، نحو بحيرة باركر، وفي أحد أطراف الشارع، واجه الحشد سياجًا حديديًا يصل ارتفاعه إلى الخصر؛ وفي الطرف الآخر، وجد الحشد مجموعة من البوابات المؤقتة، وقد تأكد فريق اتصال الاحتجاج من أن الانطباع الفوري لدى المتظاهرين هو أن هذه البوابات ستسمح للشرطة باحتوائهم والسيطرة عليهم، وقد قام فريق اتصال الاحتجاج بإرسال هذه المعلومات إلى قادة الشرطة الذين سمحوا للمتظاهرين بإدارة هذه البوابات بأنفسهم لإزالة مخاوفهم.

وبعد تجمع المتظاهرين في منطقة بحيرة باركر، كان هناك عدد من الأفراد الذين قالوا: "لا ينبغي أن يكون هذا السياج هنا، يجب أن يُسمح لنا بالذهاب إلى هناك والاحتجاج". وبدا للبعض سؤال حول شرعية قيام الشرطة ببناء هذا السياج الكبير[109].

وبعد ذلك بوقت قصير، شق "باتريك ستريتر" مندوب الحزب الليبرالي الديمقراطي طريقه إلى الحشد وبدأ في مخاطبة المتظاهرين، وقد أثار وجوده ردود فعل غاضبة من

(108) Gorringe, Hugo, Clifford Stott, and Michael Rosie., Op.Cit, pp.115117-.

(109) Gorringe, Hugo, Clifford Stott, and Michael Rosie., Op.Cit, pp.117118-.

قطاعات من الجمهور، في ذلك الوقت وقف ضباط فريق اتصال الاحتجاج في المنطقة المجاورة مباشرة لكنهم لم يتدخلوا، وبعد تقييم الوضع بسرعة، اتصلوا بقادة الشرطة وطلبوا منهم "عدم القيام بأي شيء" خوفًا من تصاعد التصورات المتعلقة بعدم شرعية الشرطة، وقد أدرك قادة الشرطة حينئذٍ التأثير السلبي المحتمل لإرسال قوات نظامية داخل الحشد لإخراج "باتريك ستريتر"، وقد لاحظ فريق اتصال الاحتجاج بعد ذلك أنه بعد أن تعرض لبعض المضايقات أصر أعضاء الحشد الآخرون على السماح له بالتحدث.

خلال هذه الحادثة، شعر قادة الشرطة أن الدراسات النظرية حول سيكولوجية الحشود منطقية، وأن الحشد قادر على التنظيم الذاتي، ولكن الأهم من ذلك هو أن فريق اتصال الاحتجاج قد "قُبل من الجمهور" وأنهم قادرون على التحرك من خلاله دون عائق أو تهديد.

وقد كان الحدث الأخير حين شق المتظاهرون طريقهم نحو مقر مؤتمر الحزب الليبرالي الديمقراطي، وعندما تجمع المتظاهرون خارج البوابات تعرضوا لبعض مندوبي الحزب بمضايقات لفظية، وعلى إثر ذلك قامت الشرطة بنشر وحدات النظام العام (ذوي السترات الصفراء) على المدخل لفرض طوق أمني.

وقد تجلت الشرعية الواضحة والقبول لفريق اتصال الاحتجاج في قدرتهم على إبعاد مجموعة الاحتجاج قليلاً عن مدخل المؤتمر، حيث تحرك فريق اتصال الاحتجاج بين الحشد موضحًا لهم السبب في الإجراءات التي قامت بها الشرطة، وقد لوحظ حينئذٍ أن مجموعة من الذين اعترضوا تم حثهم على الانسحاب من قبل الناشطين المتطرفين في الحشد، بما في ذلك بعض الذين كان من المستحيل الوصول إليهم في السابق، ولكنهم كانوا منخرطين مع فريق اتصال الاحتجاج على أرض الواقع[110].

ومع الوقت بدأ فريق اتصال الاحتجاج في اكتساب الثقة وتكوين سمعة طيبة لدى كل من الحشد وزملائهم في الشرطة، الأمر الذي سمح لهم بالتفاوض على الحلول وفهم طبيعة الوضع فهمًا أكثر دقة.

وفي الصباح تجمعت مظاهرة أكبر وأكثر تنوعًا في حديقة "ديفونشاير" وكان فريق اتصال الاحتجاج حاضرًا منذ البداية؛ حيث اختلط مع الحشد الذي بلغ نحو 4000 شخص، ووزع منشورات وتحدث مع الناس حول أدوارهم، ولم يكن هناك سوى عدد قليل من ضباط وحدة النظام العام (ذوي السترات الصفراء) وكان لديهم تعليمات بعدم مغادرة شاحناتهم، وعندما ظهر "باتريك ستريتر" مجددًا حاول الحديث في مكبر الصوت وإثارة العداء، فقام فريق اتصال الاحتجاج بتأمين خروجه بعيدًا، وحثوا المتظاهرين الغاضبين على عدم إعطائه قدرًا كبيرًا من الاهتمام والعودة إلى المنطقة الخضراء.

(110) Ibid, pp.118119-.

وقد شعرت الشرطة لأول مرة بأنهم موجودون داخل الحشد، يستمعون إليهم ويشعرون بهم ويفسرون التأثير الذي تحدثه تصرفاتهم بهم، فضلاً عن حصولهم على المعلومات حول سلوك الحشد في الوقت الفعلي[111].

وكانت ذروة التظاهرة يوم السبت عندما أشعلت بعض المشاعل وسط حشد كثيف في بحيرة باركر وقفز أحد المتظاهرين وهو يحمل شعلة مضيئة فوق الحاجز الحديدي المحيط بموقع الاحتجاج وركض نحو مكان انعقاد المؤتمر؛ حيث تم القبض عليه على الفور، وعلى الرغم من قيام البعض بإطلاق صافرات وصيحات الاستهجان، إلا أنه لم تكن هناك محاولة حقيقية أخرى لاختراق خطوط الشرطة، وقد قرر فريق اتصال الاحتجاج العمل على عدم تكرار هذا الأمر مرة أخرى وشقوا طريقهم عبر الحشد للتحدث مع شابين ملثمين يرقصون بالمشاعل، ومع اقتراب اثنين من ضباط الاتصال منهم اندفع الناس لرؤية ما يحدث وتصويره، حيث قام الضابطان بالانخراط معهم في حوار لطيف، مشيرين إلى مخاطر النيران المشتعلة على باقي أفراد الحشد، وقد استجابوا لذلك ولم يتم إشعال أي مشاعل أخرى.

وأكد حدث آخر فوائد الاتصال، عندما انفصلت مجموعة من النشطاء عن المسيرة وقاموا باحتلال رمزي لبعض المحلات التجارية في الشوارع الرئيسة، وقد لعب فريق اتصال الاحتجاج دورًا فعالاً في منع تصعيد إجراءات الشرطة ضدهم؛ حيث كانت قوات وحدة النظام العام في حالة تأهب بسبب الضغط المستمر خلال اليومين الماضيين، وكان الأمر المثير للقلق عندما بدأ أحد المتظاهرين في تشويه جدار على مرأى من الدائرة التلفزيونية المغلقة لمركز القيادة، وعندما أصدر قائد الشرطة أوامره إلى وحدة النظام العام القريبة بالدخول إلى المنطقة لاعتقال الشخص الذي يشوه الجدار، سارعت إحدى ضابطات فريق اتصال الاحتجاج بتوضيح أن الكتابة على الجدار تم رسمها بالطباشير وليس بالرش الملون؛ حيث اقتربت من الفنانة الشابة التي قامت على الفور بمسح الطباشير عن الحائط، وقد انتهى الاحتجاج وديًا بعد ذلك؛ حيث بدا أن معظم الناس يشعرون أن أصواتهم قد سُمعت.

وتجدر الإشارة إلى أن نشر ضباط الاتصال في الاحتجاجات يأتي كجزء من تحرك المملكة المتحدة الأوسع نحو الشرطة الاستباقية القائمة على الحوار، وأن استراتيجية الاتصال في شيفيلد قد وفرت نموذجًا تجريبيًا يمكن اعتماده وتعميمه.

وقد بدا واضحًا أن فريق اتصال الاحتجاج يقدم معلومات عالية الجودة على مستوى الأرض لا يمكن للقادة الوصول إليها بوسائل أخرى، وقد مكنت هذه المعرفة من إجراء تقييمات مستمرة للحالة الأمنية ساعدت على إدارة الحشود بشكل استباقي، ومع ذلك

(111) Ibid, pp.120121-.

يبدو أن إسهاماتهم الرئيسة تكمن في قدرتهم على التخفيف من ميل الشرطة إلى التدخل وتصحيح افتراضات الشرطة وتصوراتها المسبقة.

ولكن كان هناك أسئلة مهمة حول كيفية تطبيق هذا النموذج التجريبي على الاحتجاجات الأكبر حجمًا، والأكثر تطرفًا، أو الأكثر تنقلاً في مواقع مختلفة؛ حيث كان حشد شيفيلد (الذي لم يتجاوز 5000 شخص) في منطقة جغرافية صغيرة نسبيًا جعلت الضباط الـ 12 المنتشرين في فريق اتصال الاحتجاج مرئيين ويمكن الوصول إليهم طوال الوقت. ونظرًا للحاجة إلى الاختلاط بالناس والمخاوف بشأن سلامة الضباط وسط الحشد، هناك تساؤلات جدية بشأن مدى جدوى هذا التكتيك في أحداث أخرى. علاوة على ذلك، لا يزال من غير الواضح كيف يمكن أن ينجح هذا التكتيك وسط الاحتجاجات الكبيرة التي قد تحدث في العواصم مثل لندن.

ومع ذلك فإن التركيز على التواصل مع الحشد والشرطة الاستباقية قد يفسر جزئيًا سبب نجاة جنوب يوركشاير من أعمال الشغب التي انتشرت عبر مدن إنجليزية أخرى في صيف عام 2011[112].

(112) Gorringe, Hugo, Clifford Stott, and Michael Rosie., Op.Cit, pp.121124-.

الخاتمة:

تناولت الدراسة موضوع "**الحوار والتفاوض في إدارة الحشود في التظاهرات**" وهو من الموضوعات المهمة في ظل تحول بعض التظاهرات حول العالم من الطابع السلمي إلى الجنوح للعنف نتيجة لعدم إدارتها بشكل جيد نظرًا لعدم فهم سيكولوجية الحشود.

وقد تناول الباحث موضوع الدراسة من خلال **مبحثين**: تناول في **المبحث الأول** إدارة الحشود في التظاهرات، موضحاً سيكولوجية الحشود في التظاهرات، ومفهوم الحوار والتفاوض الأمني، والسمات والمهارات التفاوضيّة، واستعرض في **المبحث الثاني** بعض التجارب الدولية في إدارة الحشود في التظاهرات، موضحًا التجارب السويدية، والكندية، والبريطانية.

وتم توصل الباحث من خلال الدراسة إلى عدد من النتائج والتوصيات من أهمها ما يلي:

أولاً - النتائج:

1- يُعد الحوار والتفاوض مع الحشود من الأدوات المهمة في إدارة التظاهرات بطريقة سلمية، فهما يسهمان في تخفيف التوترات وتوجيه الأفراد نحو سلوك يحافظ على السلامة والاستقرار، ويعبر الحوار عن عمليّة تبادل الأفكار والآراء والمعلومات بين الأفراد دون ضرورة الوصول إلى اتفاق محدد أو حلٍ معين، بينما يشير التفاوض إلى عمليّة تفاوضيّة تهدف إلى الوصول إلى اتفاق أو صفقة معينة تلبي مصالح الأطراف المشاركة.

2- تهدف عمليّة إدارة الحشود في التظاهرات إلى التوجيه السلمي للمتظاهرين والحفاظ على النظام والسلامة العامة خلال فعاليات الاحتجاج، وخلق بيئة آمنة وسلمية للتعبير عن الرأي دون اللجوء إلى العنف أو التوترات الكبيرة، مع ضمان سلامة المتظاهرين والحفاظ على النظام العام، ويُعد فهم سيكولوجية الحشود أمرًا مهمًا في عمليّة إدارتها؛ إذ يساعد ذلك على التنبؤ بسلوك الحشود وفهم كيفية استجابتهم للمواقف المختلفة أثناء التظاهرات.

3- اهتم علم النفس الاجتماعي بسلوك البشر حين يتجمعون في أعداد كبيرة حيث تلاحظ اختلاف سلوكهم في هذه الحالة عن سلوكهم في حالاتهم الفرديّة، وقد حاول علماء النفس والاجتماع دراسة السلوك الجمعي والوقوف على أسبابه ودوافعه، وقد مرت هذه الدراسات بعدة مراحل تمثل كل منها نظرية مستقلة في تفسير سلوك الحشود، كما اهتموا بتصميم نماذج للحشد لوصف سلوكياته وتحركاته.

4- تشير إحدى دراسات علم النفس الاجتماعي إلى أن الحشود دائمًا ما تعتقد أنها على حق بصورة لا تخلو أحيانًا من المبالغة، وتتصور دائمًا أنها تمارس حقها القانوني في الاحتجاج، وتسيطر عليها قناعة على التوازي ناقدة للشرطة بزعم أنها تضيق عليهم، وغالبًا ما يبلغ هذا الاعتقاد مداه في لحظات اتجاه الحشد للعنف والفوضى، ومن ثمّ يسهل استثارتهم بمجرد تدخل الشرطة في المجرى العادي للأمور لفرض رؤيتها بالقوة حتى لو كان تدخلها مستظلًا بصحيح القانون، فتتصاعد سلوكياتهم في اتجاه العنف والفوضى، وأحيانًا تتأثر مجموعة بسلوك مجموعة أخرى أو تتعاطف معها فيطغى مشهد العنف على الموقف ويتعاظم.

5- يرى نموذج "الهوية الاجتماعية المفصل لسلوك الحشود" أن الاستخدام غير المتمايز للقوة من جانب الشرطة خلال حدث ما قد يؤثر سلبًا على ديناميات الحشود؛ إذ يخلق عمليات نفسية تدفعهم إلى الإخلال بالنظام العام، فمن ناحية يخلق إحساسًا بعدم شرعية أعمال الشرطة، ومن ثمّ زيادة أعداد الأفراد داخل الحشد الذين يتصورون الصراع ضد الشرطة سلوكًا مقبولًا أو مشروعًا، أي إن الاستخدام غير المتمايز للقوة من جانب الشرطة قد أحدث تغييرًا في طبيعة الهوية الاجتماعية للحشد (إحساسهم المشترك بتصنيف "نحن" في مقابل الشرطة "هم")، ومن ناحية أخرى فإن الشعور بالشرعية في معارضة الشرطة سيزيد لاحقًا من تأثير أولئك المستعدين للانخراط في مواجهة جسدية مع الشرطة، ويمكن لمثل هذه العمليات أن تجذب الحشد إلى الصراع على الرغم من أن الغالبية العظمى لم يكن لديها نية مسبقة للانخراط في الفوضى.

6- يقترح نموذج الهوية الاجتماعية المفصل لسلوك الحشود أن تكون الشرطة على علم بالظروف التي أدت إلى وجود الحشد والنيات المشروعة لأفراده، فضلًا عن تبني تكتيكات تعتمد على: (أ) تعزيز وتسهيل السلوك السلمي داخل الحشد من خلال تثقيف أنفسهم حول النيات المشروعة للمشاركين التي ينطلقون منها. (ب) التعويل على تكتيكات الحوار والتواصل والتفاوض مع الحشود قبل الحدث وأثناءه وبعده. (ج) تجنب التهديد غير المتناسب أو الاستخدام غير المتمايز للقوة؛ إذ يجب أن يكون استخدام القوة في حدود القبض على الأفراد الذين تسببوا في حادثة أو اتخذوا مواقف عدوانية وعنيفة، ولا ينبغي أن تمارس على أساس افتراض أن الحشد بأكمله يشكل تهديدًا للنظام العام.

7- تتوقف نتيجة الحوار والتفاوض على السمات والمهارات والخبرات التي يتمتع بها فريق التفاوض، ولذلك يجب الاهتمام باختيار أفراده، من حيث المكونات النفسية، والسمات الشخصية، والقدرات العقلية، مع الوضع في الاعتبار أن هناك سمات شخصية طبيعية لا يمكن تعلمها، وهناك سمات يمكن اكتسابها بالتعلم وصقلها وتنميتها بالتدريب.

8- يعد الإلمام بالتفاوض كعلم وفن ضرورة ملحة لرجل الأمن أيًا كانت وظيفته وأينما كان موقعه، فمن المستحيل أن يتم تجاهل الحاجة للتفاوض ولو من وقت لآخر؛ إذ إن عدم قدرة رجل الأمن على إدارة بعض المواقف الأمنية بطريقة سليمة قد يحول بعض المواقف الأمنية العابرة التي يتعرض لها أفراد الجهاز الأمني يوميًا إلى أزمات أمنية تهدد بتطورات لا يحمد عقباها.

9- تحول سياسات وممارسات شرطة مكافحة الشغب في الدول الغربيّة من الأسلوب القائم على المواجهة الخشنة مع الحشود إلى نموذج يستند إلى فكرة نزع فتيل العنف وتسوية النزاع، ويعتمد على جمع المعلومات والتواصل مع المتظاهرين والحوار والتفاوض معهم.

10- قامت بعض الدول الغربيّة بتطوير نموذج مستحدث للتعامل الشرطي مع الحشود في التظاهرات يعتمد على الحوار والتفاوض معها، ويرتكز إلى تجارب عمليّة أثبتت نجاحها في إدارة الحشود في التظاهرات في بعض الدول (السويد عام 2001 – كندا عامي 2001، 2002 – بريطانيا عام 2009) كما أصبح له سجل حافل واعتراف دولي كنموذج للممارسة الجيدة في إدارة الحشود في التظاهرات.

ثانيًا - التوصيات:

1- الاهتمام بصقل قدرات وتنمية مهارات رجال الشرطة في العلوم النفسية والسلوكية التي تهتم بدراسة سلوك الإنسان في المواقف المختلفة، خاصة نظريات علم النفس الاجتماعي الحديثة التي تهتم بفهم السلوك الإنساني داخل الحشود في التظاهرات.

2- إدراج موضوعي "التفاوض الأمني – إدارة الحشود في التظاهرات" ضمن مناهج (طلاب كلية الشرطة – فرق التدريب لضباط الشرطة) على أن يتضمنا: مفهوم الحوار، مفهوم التفاوض، الفرق بين الحوار والتفاوض، السمات الشخصية للمفاوض، المهارات التفاوضيّة، موضوعات التفاوض في العمل الأمني، تكتيكات واستراتيجيات التفاوض، وأهم التجارب الدولية التي أثبتت نجاحًا في إدارتها.

3- استخدام التكتيك الشرطي المستحدث الذي يعتمد على بناء الثقة بين الشرطة والمتظاهرين ويتضمن بعض الأدوات، مثل جمع المعلومات، والمراقبة، وإجراء الحوار، والتفاوض، والذي أثبت نجاحًا عمليًا في عدد من الدول الأوروبية، وتم وضعه موضع التنفيذ الفعلي للتعامل الشرطي مع الحشود وخاصة في التظاهرات مع مراعاة ما يلي:

- تطبيق التكتيك المشار إليه تطبيقًا تدريجيًا للوقوف على مدى ملاءمته للبيئة العربيّة، في ظل تباين تعداد وثقافة ومعدلات رفاهية السكان في الدول الأوروبية التي طبق فيها، وإلى أي مدى يمكن أن تكون هذه الفوارق داعمة لنجاح النموذج في بيئته، مع إمكانية تطويره وإدخال التعديلات عليه ليتلاءم مع البيئة العربيّة.

- استحداث إدارة شرطية تختص بالحوار مع الحشود في التظاهرات على أن يتم انتقاء أعضائها بعناية ممن تتوفر فيهم السمات الشخصية والقدرات العقلية والمكونات النفسية اللازمة لذلك، مع الوضع في الاعتبار أن هناك سمات شخصية طبيعية لا يمكن تعلّمها، وهناك خصائص وصفات يمكن اكتسابها بالتعلّم وصقلها وتنميتها بالتدريب.

- التأكيد على أن يعمل ضباط الحوار قبل وبعد الأحداث الجماهيرية لإقامة علاقات طويلة الأمد قائمة على الثقة والاحترام المتبادل مع المتظاهرين.

- التأكيد على المكونات الأساسية الخمسة لضبط الحوار وهي: التفاوض، والوساطة، والبدء "اقتراح الحلول الممكنة للمشاكل"، والتواصل، والاستشعار "التقييم المستمر للتهديد الذي يتعرض له النظام العام أثناء حدث جماهيري".

قائمة المراجع

أولاً - المراجع العربيّة:

أ - المؤلفات العامة والمتخصصة:

- الخضيري، محسن أحمد. التفاوض علم تحقيق المستحيل انطلاقًا من الممكن. القاهرة: مكتبة الأنجلو المصرية، 1988.
- الخضيري، محسن. تنمية المهارات التفاوضيّة. القاهرة: الدار المصرية اللبنانية، الطبعة الأولى، 1993.
- الوزان، السيد حلمي. التدريب مدخل للتنمية البشرية في الشرطة. القاهرة: بدون دار نشر، 2009.
- الوزان، السيد حلمي. التفاوض .. كيف تكون مفاوضاً أمنياً ناجحاً ومقنعاً. بدون دار نشر، 2011.
- آندرسون، برابرة. مهارات التفاوض الاحترافي. القاهرة: مكتبة الهلال للنشر والتوزيع، 2010.
- حواش، جمال. التفاوض في الأزمات والمواقف الطارئة مع تطبيقات عمليّة. بدون دار نشر، 2005.
- روبنز، فيليب. التفاوض فن الفوز. القاهرة: دار الخلود للتراث، 2010.
- سعد الدين، أيمن. إدارة الحشود في العمل الأمني. القاهرة: بدون دار نشر، الطبعة الثالثة، 2022.
- عنب، محمد محمد محمد. التحقيق والبحث الجنائي في إدارة الأزمات والكوارث. بدون دار نشر، 2012.
- فرحات، طارق خيرت. الإنذار الأخير سيكولوجية التفاوض باستخدام الذكاء الاصطناعي. بدون دار نشر، بدون سنة نشر.
- مرعي، توفيق وبلقيس، أحمد. الميسر في علم النفس الاجتماعي. عمان: دار الفرقان للنشر والتوزيع، 1984.
- ندا، محمد عبد المنعم. كيف تصبح مفاوضًا فعالًا. القاهرة: هلا للنشر والطباعة، 2006.

ب - الرسائل العلميّة:

- حجازي، حسني عبد العزيز رزق. إدارة التفاوض في الأزمات الأمنية. القاهرة: رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، 2017.
- عثمان، أحمد محمد صالح أحمد. تطبيقات الذكاء الاصطناعي ودورها في الإدارة الأمنية للحشود. القاهرة: رسالة دكتوراة، كلية الدراسات العليا، أكاديمية الشرطة، 2022.

ج - الدراسات والبحوث:

- عبد الحليم، وليد ممدوح. آليات تنمية مهارات التفاوض لدى رجل الشرطة. القاهرة: بحث مقدم لكلية الدراسات العليا، أكاديمية الشرطة ، 2013.
- مركز بحوث الشرطة بأكاديمية الشرطة، علم التفاوض ودوره في مواجهة الجرائم الإرهابية "احتجاز الرهائن"، الإصدار التاسع والستون، 2017.

د - مقالات الدوريات:

- إبراهيم، حليم أحمد محمود. "تطبيقات علم النفس الاجتماعي في تعامل الشرطة مع الاحتجاجات"، القيادة العامة لشرطة الشارقة، دورية الفكر الشرطي 24، ع 95 (أكتوبر 2015).
- الرميضي، جمال سعد والشمري، محمد مرضي. "مهارات التفاوض الأمني الناجح"، جامعة نايف العربيّة للعلوم الأمنية، المجلة العربيّة للدراسات الأمنية 1، ع 38 (2022).
- العبودي، محسن. "نحو استراتيجية علميّة في مجال إدارة الأزمات والكوارث"، القاهرة، مجلة كلية الدراسات العليا بأكاديمية الشرطة، ع 4 (2011).
- خلف، عبد العزيز. "مهارات التفاوض"، مجلة المدير العربي، ع 151 (2000).
- سرسيق، إبراهيم محمد. "سيكولوجية الجماهير في القرآن الكريم"، اللجنة الوطنية القطرية للتربية والثقافة والعلوم، مجلة التربية، ع 29 (1978).

ثانيًا - المراجع الأجنبية:

- Challenger, Rose, et al. "Understanding crowd behaviours: Supporting evidence." Understanding Crowd Behaviours'(Crown, 2009) (2009).
- Gorringe, Hugo, Clifford Stott, and Michael Rosie. "Dialogue police, decision making, and the management of public order during protest crowd events." Journal of investigative psychology and offender profiling 9.2 (2012).
- Hogg, Michael A., and Scott Tindale, eds. Blackwell handbook of social psychology: Group processes. John Wiley & Sons (2008).
- Holgersson, Stefan. Dialogue police: experiences, observations and opportunities. National Police Board (2010).
- King, Mike. "From reactive policing to crowd management? Policing anti-globalization protest in Canada." (2014).

- La Macchia, Stephen T., and Winnifred R. Louis. "Crowd behaviour and collective action." Understanding peace and conflict through social identity theory. Springer, Cham (2016).
- Quanbin Sun, A Generic Approach to Modelling Individual Behaviours in Crowd Simulation,University of Salford, School of Built and Environment (2013).
- Reicher, Stephen, et al. "An integrated approach to crowd psychology and public order policing." Policing: an international journal of police strategies & management (2004).
- Stott, Clifford, and John Drury. "Crowds, context and identity: Dynamic categorization processes in the poll tax riot'." Human relations 53 (2000).
- Stott, Clifford, and John Drury. "The inter-group dynamics of empowerment: A social identity model." Transforming politics. Palgrave Macmillan, London (1999).
- Stott, Clifford. "Crowd psychology and public order policing: an overview of scientific theory and evidence." Submission to the HMIC Policing of Public Protest Review Team. Liverpool: University of Liverpool, UK (2009).
- Waddington, David P. "From Iron Fists to Bunches of Fives: A Critical Reflection on Dialogue (or Liaison) Approaches to Policing Political Protest." Special Issue 1 Eur. Police Sci. & Res. Bull. (2013).

جرائم غسل الأموال وأوجه خروجها عن الأحكام العامة في القانون القطري

الدكتور/ إياد هارون الدوري
أستاذ القانون الجنائي المساعد – كلية القانون – جامعة قطر

جرائم غسل الأموال وأوجه خروجها عن الأحكام العامة في القانون القطري

الدكتور/ إياد هارون الدوري
أستاذ القانون الجنائي المساعد – كلية القانون – جامعة قطر

المُلخَّص

تتمحور هذه الدراسة حول جرائم غسل الأموال، وتحديدًا حول خروجها عن الأحكام العامة، وتكمن إشكالية هذا البحث في كون جرائم غسل الأموال تتميز بخصوصية استوجبت خروج المشرع الجنائي في القوانين المقارنة (ومنهم المشرع القطري) عن الأحكام العامة المقررة في قوانين العقاب، وهنا تبرز الإشكالية المتمثلة في الخلط واللبس الذي يمكن الوقوع به بين تطبيق الأحكام العامة الواجب تطبيقها على جميع الجرائم، وبين خروج جرائم غسل الأموال عن تلك الأحكام العامة، سواء من حيث أحكام الاشتراك أم الشروع أم الارتباط أم سريان القانون من حيث المكان.

اعتمدنا المنهج الوصفي التحليلي المقارن، فجاء البحث في مقدمة وثلاثة مباحث وخاتمة، حيث تناولنا في المقدمة موضوع الدراسة وإشكاليتها وأهدافها والدراسات السابقة ومنهجية البحث، أما المبحث الأول فتناولنا فيه ماهية جرائم غسل الأموال، وفي الثاني بحثنا الإطار التشريعي لها، وتناولنا في المبحث الثالث أوجه خروج هذه الجرائم عن القواعد العامة، ثم اختتمنا البحث بجملة من النتائج والتوصيات، أهمها اقتراح إعادة النظر بأحكام المادة 17 من قانون العقوبات القطري، وذلك بشمول جرائم غسل الأموال بمبدأ عالمية النص الجنائي، والتوصية باقتراح إعادة النظر بأحكام المادة 37 من قانون العقوبات القطري بشأن عقوبة الشخص المعنوي، والتوصية باستبعاد التقدم الجنائي في هذه الجرائم، والتوصية بإعادة صياغة نص الفقرة 4 من المادة 2 من قانون مكافحة جرائم غسل الأموال وتمويل الإرهاب.

الكلمات المفتاحية: جرائم غسل الأموال، التشريعات القطرية، مكافحة الفساد

ABSTRACT

Laundering Crimes, specifically on their departure from the general provisions

Dr .Ayad Haroon Al-Douri
Assistant Professor of Criminal Law - Qatar University

This study focuses on money laundering crimes, specifically on their departure from the general provisions. The problem that this research revolves around is the fact that money laundering crimes are characterized by a specificity that required the criminal legislator in similar laws (including the Qatari legislator) to depart from the general provisions specified in the penal laws, and here the problem arises represented by the confusion. And the confusion that may occur between the application of the general provisions that must be applied to all crimes, and the departure of money laundering crimes from those general provisions, whether in terms of the provisions of participation (taking part-in), attempt, association, or the application of the law in terms of place.

We adopted the comparing descriptive analytical approach. The research included an introduction, three parts, and a conclusion. In the introduction, we talk about the subject of the study, its problems, its objectives, previous studies, and the research procedure. In the first section, we discussed the nature of money laundering crimes and in the second, we disclosed the legislative frame for them. In the third section, we discussed parts of these crimes are out of the general rules. The research concluded with recommendations, including amending Article 17 of the Qatari Penal Code to include money-laundering crimes, amending Article 37 to address legal punishment, removing criminal progress in these crimes, and remaking Paragraph 4 of Article 2 of the Law on Combating Money Laundering and Terrorist Financing to remove legislative excess.

Keywords: laundry Money Crimes , Qatari Legislation , Anti-corruption

المقدمة:

تُشكل مكافحة جرائم غسل الأموال حجر الزاوية في مكافحة جرائم الفساد بشكل عام، وتُشكل في الوقت ذاته، قطعًا للطريق أمام إتمام دورة الفساد التي تبدأ بالجريمة التي يُتحصل منها على الأموال الفاسدة، مرورًا بإلباسها ثوب الشرعية من خلال جريمة غسل الأموال، انتهاءً بتضخم الذمم المالية للفاسدين تحت ما يسمى بجرائم الكسب غير المشروع، وقد سبق لنا البحث في موضوع ضرورة تجريم الكسب غير المشروع في القانون القطري من خلال بحث سابق ومنشور، وفي بحثنا هذا نكمل الطريق في مجال مكافحة الفساد؛ حيث نبحث في جرائم غسل الأموال وتحديدًا أوجه خروجها عن الأحكام العامة في القانون القطري.

إشكالية البحث:

تكمن إشكالية البحث في كون جرائم غسل الأموال تتميز بخصوصية استوجبت خروج المشرع الجنائي في القوانين المقارنة (ومنهم المشرع القطري) عن الأحكام العامة المقررة في قوانين العقاب، وهنا تبرز الإشكالية المتمثلة في الخلط واللبس الذي يمكن الوقوع به بين تطبيق الأحكام العامة الواجب تطبيقها على جميع الجرائم، وبين خروج جرائم غسل الأموال عن تلك الأحكام العامة، سواء من حيث أحكام الاشتراك أم الشروع أم الارتباط أم سريان القانون من حيث المكان.

أهداف البحث:

يهدف البحث من جانب إلى شرح أحكام جرائم غسل الأموال وتحديد أوجه خروجها عن الأحكام العامة في القانون القطري، ومن الجانب الآخر يهدف إلى تحديد أحكام نتمنى فيها على المشرع القطري الخروج فيها عن الأحكام العامة في مثل هذا النوع من الجرائم ولم يأخذ بها.

الدراسات السابقة:

كتب الكثير عن جرائم غسل الأموال في الفقه المقارن وكذلك في القانون القطري، وقد أشرفنا أو ناقشنا بعض منها، على سبيل الذكر

- إشرافنا على رسالة ماجستير موسومة بعنوان "معوقات مكافحة جرائم الفساد في القانون القطري" للباحثة شريفة الخليفي (2018) جامعة قطر.

رسالة ماجستير أشرفنا عليها وتضمنت معوقات مكافحة جرائم غسل الأموال وسبل تذليلها من أجل الحد منها.

- إشراف مشترك (بشير زغلول، إياد الدوري) على رسالة ماجستير موسومة بعنوان "تمويل الإرهاب والإجراءات القانونية لمكافحته وفقًا للتشريعات القطرية"، محمد جبر النعيمي، رسالة مقدمة إلى كلية القانون جامعة قطر 2020.

تهدف الدراسة إلى تعريف تمويل الإرهاب في القانون الدولي والتشريعات الوطنية والمقارنة بينهما، والتعرف على مصادر تمويل الإرهاب وعلاقتها بغسل الأموال والجريمة المنظمة وغيرها من الجرائم الأخرى، وبيان الإطار القانوني للتعاون الدولي والإقليمي لمنع تمويل الإرهاب، والتعرف على التنظيم القانوني الوطني لتجريم تمويل الإرهاب والعقاب عليه، وبيان الإجراءات الوقائية والإجرائية لمنع عمليات تمويل الإرهاب.

- مناقشتنا رسالة ماجستير موسومة بعنوان "جريمة غسل الأموال في ضوء قانون مكافحة غسل الأموال رقم 20 لسنة 2019 وتمويل الإرهاب والمعايير الدولية لمكافحة غسل الأموال" للباحث حامد القحطاني (2020) جامعة قطر.

تمحورت الدراسة حول سياسة المشرع القطري في مجال مكافحة الفساد، وكذلك المعايير الدولية في هذا الشأن.

ومن الدراسات الأخرى نشير إلى التالي:

- جرائم غسل الأموال في القانون القطري، سامي الرواشدة، بحث باللغة الإنجليزية منشور:

Crime of money laundering in Qatari Law: Definition and Elements: A Comparative Study" (2020) Vol. 23, Issue 5, Journal of Legal, Ethical and Regulatory Issues) Scopus, Q2). 2–

تمحورت الدراسة حول تعريف جرائم غسل الأموال في القانون القطري وبيان عناصرها، وركزت الدراسة على الإطار النظري لتعريف جرائم الفساد، وكذلك تحديد الأحكام العامة لها وبيان عناصرها.

- المسؤولية الجنائية عن جرائم غسل الأموال والإطار التنظيمي لمكافحتها في القانون القطري، بحث باللغة الإنجليزية منشور:

Framework Criminal Liability for the Crime of Money Laundering and the Regulator" for Combating It in Qatari Law" (2022) Vol. 25, Special Issue 1, Journal of Legal, (Ethical and Regulatory Issues) Scopus, Q2

تناولت الدراسة المسؤولية الجنائية الناجمة عن جرائم غسل الأموال والإطار التشريعي لمكافحتها في القانون القطري، وتركزت حول القواعد والأحكام العامة في هذا النوع من الجرائم.

- مكافحة غسل الأموال وتمويل الإرهاب وجهود دولة قطر، هاشم السيد، دار الوتد، 2020، قطر.
كتاب يتناول بشكل عام جهود دولة قطر في مكافحة جرائم غسل الأموال وتمويل الإرهاب ويمكن تصنيفه أنه يدخل ضمن مؤلفات جرائم الفساد.
- جريمة غسل الأموال في التشريع القطري، منصور القحطاني، رسالة ماجستير، 2008، كلية الحقوق- جامعة القاهرة.
تناولت الدراسة مصطلح غسل الأموال كجريمة جنائية مستحدثة في الفقه والوثائق الدولية والإقليمية وفي التشريعات المقارنة وأساس تجريم غسل الأموال ووسائل غسل الأموال والتعاون الدولي في مجال مكافحتها، وركزت الدراسة على الأحكام العامة لهذا النوع من الجرائم.

أما بشأن بحثنا هذا، فإنه ينفرد ويتميز عما سبقه من دراسات سابقة في أنه يركز ويبحث أوجه خروج هذا النوع من الجرائم عن تلك الأحكام العامة التي كانت قد تناولتها الدراسات السابقة المشار إليها أعلاه.

منهجية البحث:

اعتمدنا في بحثنا هذا المنهج الوصفي التحليلي، أما بالنسبة للمنهج الوصفي فتم توظيفه في وصف وشرح الأحكام العامة لجرائم غسل الأموال القانون القطري وفقًا لأحدث التشريعات الصادرة بهذا الشأن، وكذلك وصفها في القانون المقارن، أما المنهج التحليلي فتم اعتماده لتحليل تلك الأحكام بشكل دقيق ومعمق للوقوف على أوجه خروجها عن الأحكام العامة في قانون العقوبات.

المبحث الأول
في ماهية جرائم غسل الأموال

تقديم:

ذهب بعض الشراح[1] إلى أن ظاهرة غسل الأموال تعود إلى الحضارات القديمة، لا سيما إبان الإمبراطورية الصينية، فكان التجار يحاولون إخفاء أموالهم عن الحكام خشية مصادرتها فكانوا يلجؤون إلى استثمارها في مشاريع أخرى في المناطق البعيدة أحيانًا خارج الإمبراطورية، بيد أننا لا نتفق مع من ذهب إلى هذا المذهب في التأصيل التاريخي، بسند من القول، إن الأموال في الحالة المذكورة آنفًا لم تكن متحصلات جريمة بل هي عملية لحماية أموال مشروعة، وبالتالي لا يمكن القول إنها عملية غسل للأموال بل إنها تخرج كليًا عن مفهوم جرائم غسل الأموال، ويذهب بعض الشُّراح إلى أن جذور جرائم غسل الأموال تعود إلى شخص يدعى (Meyer Lansky) كان يمثل حلقة الوصل بين المافيا الأمريكية والمافيا الإيطالية لإدخال قوات الحلفاء إلى جزيرة صقيلية[2]، لكن الرأي الراجح لدينا أن جذور جرائم غسل الأموال أو تسمية غسل الأموال أو تبييض الأموال تعود إلى ثلاثينيات القرن الماضي، وتحديدًا إلى عصابات المافيا الشهيرة؛ حيث تم القبض على زعيمها ويدعى (آل كابون) سنة 1931 بالتهمة الوحيدة التي أمكن إثباتها عليه وهي التهرب من دفع الضرائب، بعد هذا التاريخ توجهت عصابات المافيا لتأسيس أعمال مشروعة تستخدمها لتمرير الأرباح الهائلة الناجمة عن العمليات الإجرامية التي تقوم بها، وكان منها تأسيس وشراء محلات التبييض الآلية أو مؤسسات التنظيف، لإدخال الأموال المشبوهة للتغطية على مصدرها، ومنذ ذلك الحين أطلق على العمليات التي تقوم بها المؤسسات الإجرامية لإخفاء مصدر الأموال غير المشروعة وتحويلها إلى أموال تظهر وكأنها مشروعة، عمليات تبييض أو غسل الأموال[3].

تقسيم:

نتناول في هذا المبحث ماهية جرائم غسل الأموال، حيث قسمنا المبحث إلى مطلبين نتناول في المطلب الأول تعريف جرائم غسل الأموال، وفي المطلب الثاني علة تجريم غسل الأموال وخصائصها وآثارها.

(1) الضمور، باسل عبد الله، غسل الأموال في المصارف، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض، (2013) ص22.
(2) الوكيل، محمد، مكافحة جريمة غسل الأموال في المملكة العربية السعودية، مكتبة القانون والاقتصاد، الرياض(2015) ص18.
(3) إسماعيل، سمر فايز، تبييض الأموال، منشورات زين الحقوقية، لبنان (2010) ص36.

المطلب الأول: تعريف جرائم غسل الأموال

سيقت العديد من التعريفات لجرائم غسل الأموال سواء في الفقه المقارن أم الاتفاقيات الدولية أم القوانين المقارنة؛ حيث عرفتها لجنة العمل المالي لغسل الأموال المعروفة باسم (F.A.T.F) التي أنشأتها قمة الدول الصناعية السبع عام 1989 بأنها (تحويل الممتلكات مع العلم بأن مصدرها جريمة بهدف إلغاء أو إخفاء الأصل غير المشروع لتلك الممتلكات، أو مساعدة أي شخص مشترك في ارتكاب تلك الجريمة لتجنب العوائق القانونية لأعماله وإلغاء أو إخفاء الطبيعة الحقيقية ومصدر ومكان وحركة وحقوق أو ملكية الممتلكات مع العلم بأن مصدرها جريمة أو من شخص ساهم في ارتكابها)[4]، وعرفها قانون عائدات الجريمة البريطاني لعام 2002 بأنها "إخفاء أو تمويه أو تحويل أو نقل أو إزالة الممتلكات الإجرامية خارج نطاق الولاية القضائية أو الدخول أو المشاركة في ترتيب يسهل الحصول على الممتلكات الإجرامية أو الاحتفاظ بها أو استخدامها أو السيطرة عليها أو اكتساب أو استخدام أو حيازة الممتلكات الإجرامية"[5]. أما المشرع الأسترالي فقد اختط نهجًا مختلفًا في تعريف الجريمة فعرفها بالقول "غسيل الأموال هو نشاط إجرامي يحدث عندما تشكل الأموال أو الممتلكات عائدات الجريمة أو عندما يكون هناك خطر أن تصبح هذه الأموال أو الممتلكات أداة للجريم"[6].

المشرع القطري بدوره لم يعرف جريمة غسل الأموال، واكتفى بتحديد صورها، وذلك بموجب المادة 2 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019؛ حيث جاء في مطلعها أنه "يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية"، وذكر عدة أفعال سيتم استعراضها لاحقًا وبشكل مفصل.

كذلك الحال بالنسبة للمشرع المصري، فلم يعرفها واكتفى في الفقرة (ب) من المادة الأولى من قانون مكافحة غسل الأموال رقم 80 لسنة 2002 بالقول، إن المقصود بغسل الأموال هو "كل فعل من الأفعال المنصوص عليها في المادة 2 من هذا القانون" وكانت المادة

(4) الأشقر، منى، تبيض الأموال الناتجة عن الاتجار غير المشروع بالمخدرات/ مركز المعلوماتية القانونية –الجامعة اللبنانية (1995)، ص25.

(5) LexisNexis website, https://www.lexisnexis.co.uk/legal/guidance/what-types-of-offences-under-the-proceeds-of-crime-act-2002-poca-2002-should-lawyers-who-are-acting-in

(6) Crime of money laundering in Qatari Law: Definition and Elements: A Comparative Study" Sami Hamdan Al-rawashdah (2020) Vol. 23, Issue 5, Journal of Legal, Ethical and Regulatory Issues)Scopus, Q2) page(3)

2 من القانون ذاته قد حددت أفعالاً اعتبرتها غسلاً للأموال (للتفصيل انظر الهامش)[7].

أما المشرع الفرنسي فقد عرف جريمة غسل الأموال في الفقرة 1 من المادة 324 من القانون الجنائي الفرنسي لعام 1994 وكذلك في المادة الأولى من قانون مكافحة غسل الأموال بموجب القانون المعدل لسنة 1996، أنها "تسهيل بكل الوسائل للتبرير الكاذب لمصدر الأموال والدخول لمرتكب جناية أو جنحة الذي أمده بفائدة مباشرة أو غير مباشرة، ويعتبر أيضًا من قبيل غسيل الأموال المساهمة في عملية توظيف أو إخفاء أو تحويل العائد المباشر أو غير المباشر لجناية أو جنحة"[8].

أما في مجال الفقه، فمنهم من عرفها بأنها "إخفاء حقيقة الأموال المستمدة من طريق غير مشروع عن طريق القيام بتصديرها أو إيداعها في مصارف دول أخرى، أو نقلها أو إيداعها أو توظيفها أو استثمارها في أنشطة مشروعة، للإفلات بها من الضبط والمصادرة[9]، بينما ذهب البعض إلى تعريفها بأنها "إضفاء الصفة الشرعية بطريقة ما على الأموال النقدية المستمدة من العائدات غير المشروعة[10]، ومنهم من عرفها بأنها "مجموعة العمليات المالية المتداخلة التي تتم داخل الدولة أو خارجها لإخفاء حقيقة الأموال أو طمس مصدرها غير المشروع وإظهارها في صورة أموال متحصلة من مصدر مشروع"[11] وبدورنا نتفق مع التعريف لإنه يشمل مراحل جرائم غسل الأموال وعناصرها وغايتها .

(7) انظر نص المادة 2 من قانون مكافحة غسل الأموال المصري رقم 80 لسنة 2002، حيث نصت على أنه "يعد مرتكبًا لجريمة غسل الأموال كل من علم أن الأموال أو الأصول متحصلة من جريمة أصلية وقام عمدًا بأي مما يلي:
أ. تحويل متحصلات أو نقلها، وذلك بقصد إخفاء المال أو تمويه طبيعته أو مصدره أو مكانه أو صاحبه أو صاحب الحق فيه أو تغيير حقيقته أو الحيلولة دون اكتشاف ذلك أو عرقلة التوصل إلى مرتكب الجريمة الاصلية. ب. اكتساب المتحصلات أو حيازتها أو استخدامها أو إدارتها أو حفظها أو استبدالها أو إيداعها أو ضمانها أو استثمارها أو التلاعب في قيمتها أو إخفاء أو تمويه الطبيعة الحقيقية لها أو لمصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها

(8) France Penal Code Article 324- (قانون العقوبات الفرنسي النافذ)
(Act no. 96392- of 13th May 1996 Article 1 Official Journal of 14th May 1996) Money laundering is facilitating by any means the false justification of the origin of the property or income of the perpetrator of a felony or misdemeanor, which has brought him a direct or indirect benefit. Money laundering also comprises assistance in investing, concealing or converting the direct or indirect products of a felony or misdemeanor.
Money laundering is punished by five years' imprisonment and a fine of €375,000

(9) العمري، عزت محمد، جريمة غسل الأموال، ط1، دار النهضة العربية، مصر، (2006) ص13.

(10) العريان، محمد علي، عمليات غسيل الأموال وآليات مكافحتها، دار الجامعة الجديدة للنشر، الإسكندرية، (2005) ص36.

(11) الدليمي، مفيد نايف، غسيل الأموال في القانون الجنائي، دار الثقافة للنشر والتوزيع،ط1، عمان، الأردن، (2005) ص32.

المطلب الثاني: علة تجريم غسل الأموال وخصائصها وآثارها

تركيزًا على موضوع البحث فإننا سنذكر بإيجاز شديد علة وخصائص وآثار هذا النوع من الجرائم، أما من حيث العلة التي تقف وراء تجريم المشرع لهذه الجرائم فإن الأموال محل الواقعة متحصلة عن جريمة هذا من جانب، ومن الجانب الآخر أنها تمثل تمويهًا وتسترًا وإخفاء لهذه الأموال غير المشروعة، وما يجب كشفه وعدم إتاحة الفرصة لمرتكب الجريمة للتمتع بثمرة جريمته[12]، أخيرًا فإنها تشكل ديمومة ومغذيًّاً لاستمرار جرائم الفساد من خلال تدوير هذه الأموال في أعمال فساد جديدة.

أما من حيث خصائصها فيمكن إجمالها باختصار، بأنها من الجرائم الاقتصادية، وأنها جريمة منظمة عابرة للحدود، وأخيرًا أنها من الجرائم التابعة لجريمة أصلية[13].

أما من حيث الآثار[14] فإن لها آثار اقتصادية مدمرة سواء على الاقتصاد الكلي للبلد أم على التضخم أم تشويه هيكل الاقتصاد أم على الاستثمار وغيرها من الآثار الاقتصادية، كذلك لجرائم غسل الأموال آثار اجتماعية وأخلاقية وسياسية وأمنية لا يتسع المقام لذكرها .

المبحث الثاني
الإطار التشريعي لجرائم غسل الأموال

تقديم:

نتناول في هذا المبحث الإطار التشريعي لجرائم غسل الأموال في القانون القطري من حيث أركانها وعقوبتها، ثم نستعرض موقف الاتفاقية المرجعية في هذا المجال وهي الاتفاقية الأممية لمكافحة الفساد لسنة 2003 وبيان موقفها من جرائم غسل الأموال.

تقسيم:

نتناول في المطلب الأول الإطار التشريعي لمكافحة جرائم الفساد في القانون القطري، وفي المطلب الثاني نبحث موقف الاتفاقية الأممية لمكافحة الفساد لسنة 2003 بشأن تجريم غسل الأموال في التشريعات الوطنية.

(12) جاسم، عمار باسل، جريمة غسل الأموال في القانون العراقي، عالم المعرفة للكتاب، بغداد، (2011) ص12.

(13) نبيلة، قيشان، الدور الوقائي للبنك في مكافحة تبيض الأموال، دار الأيام للطباعة والنشر، عمان،(2017) ص16.

(14) عبود، سالم محمد ظاهرة، غسيل الأموال –المشكلة والآثار، دار الدكتور للعلوم الإدارية والاقتصادية، بغداد الطبعة الثانية، (2013) ص65 وما بعدها

المطلب الأول: الإطار التشريعي لجرائم غسل الأموال في القانون القطري

نبحث في هذا المطلب الإطار التشريعي لجرائم غسل الأموال في القانون القطري، وذلك من حيث الأركان والعقوبة المقررة لها، وعليه سوف نخصص الفرع الأول للركن المفترض لها، وفي الثاني نبحث الركن المادي، وفي الثالث نبحث الركن المعنوي، وفي الفرع الأخير نبحث عقوبتها سواء على الشخص الطبيعي أم الاعتباري.

ابتداءً تجب الإشارة إلى أن القانون رقم 20 لسنة 2019" تميز عن سابقه من التشريعات المنظمة لمكافحة غسل الأموال في قطر، بأنه احتوى عددًا من المميزات التي ستمكن دولة قطر من ضمان معالجة جرائم غسل الأموال وتمويل الإرهاب بفعالية وكفاءة، وهذه الميزات المدرجة في القانون هي توسيع تعريف الجرائم الأصلية، مصدر الأموال غير المشروعة، لتشمل جميع الجنايات والجنح، تطبيق الإفصاح الجمركي، حيث يلتزم المسافر بالإفصاح عما بحوزته من النقد الأجنبي، وتعزيز دور الهيئة الوطنية لجنة مكافحة غسل الأموال وتمويل الإرهاب؛ ما يسمح لها بتقييم الوضع الوطني لنظام مكافحة غسل الأموال والإشراف على حسن سير أعماله"[15].

نصت المادة 2 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019 على أنه " يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية

1. تحويل الأموال أو نقلها مع العلم بأنها متحصلات جريمة أو أي من أفعال الاشتراك في هذه الجريمة، بقصد إخفاء أو تمويه المصدر غير المشروع لتلك الأموال، أو مساعدة أي شخص قام بارتكاب هذه الجريمة على الإفلات من العواقب القانونية لأفعاله.
2. إخفاء أو تمويه الطبيعة الحقيقية للأموال أو مصدرها أو مكانها أو طريقة التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأنها متحصلات جريمة.
3. اكتساب الأموال أو حيازتها أو استخدامها مع العلم وقت تسلمها أنها متحصلات جريمة.
4. الاشتراك أو الارتباط أو التواطؤ أو المساعدة أو التحريض أو التسهيل أو تقديم المشورة أو التعاون أو المساهمة أو التآمر في ارتكاب أو الشروع في ارتكاب أي من الأفعال المحددة في هذه المادة.

وتعد جريمة غسل الأموال جريمة مستقلة عن الجريمة الأصلي. وعند إثبات أن الأموال متحصلات جريمة، لا يشترط أن يكون قد تمت إدانة الشخص بارتكاب جريمة أصلية. ولا تحول معاقبة الأشخاص الذين يرتكبون الجريمة الأصلية دون معاقبتهم على جريمة غسل الأموال".

(15) "Criminal Liability for the Crime of Money Laundering and the Regulator Framework for Combating It in Qatari Law" Sami Hamdan Al-rawashdah (2022) Vol. 25, Special Issue 1, Journal of Legal, Ethical and Regulatory Issues Scopus, Q2, page 16

من خلال قراءة النص سالف الذكر، نخلص إلى أن قيام جريمة غسل الأموال يتطلب ثلاثة أركان، ركن المحل والركن المادي والركن المعنوي، كذلك نستدل من مراجعتنا للنص ذاته، أن المشرع القطري قرر بعض الأحكام الخاصة لهذه الجريمة، وهو ما سيتم تناوله تباعًا في المباحث التالية.

الفرع الأول: الركن المفترض (المحل)

جريمة غسل الأموال تشترط ابتداءً أن تكون الأموال محل الجريمة غير مشروعة، أي متحصلة عن جريمة، وهنا يكمن جوهر التجريم، فسلوك الإخفاء أو التمويه أو التملك أو الحيازة لتلك الأموال ما كان ليشكل جريمة لولا أنه يقع على أموال متحصلة أساسًا من جريمة، وعليه إثبات أن الأموال متحصلة عن جريمة ركن لازم لقيامها، وهذا ما أكدته الفقرات الأولى والثانية والثالثة من نص المادة 2 من قانون مكافحة غسل الأموال وتمويل الإرهاب؛ حيث نجد أن المشرع القطري اشترط أن تكون الأموال متحصلة عن جريمة.

يقصد بمصطلح (متحصلات الجريمة) طبقًا لنص المادة الأولى من القانون ذاته هو " أي أموال ناتجة أو تم الحصول عليها بصورة مباشرة أو غير مباشرة، من خلال ارتكاب إحدى الجرائم الأصلية، وتشمل ما تدره هذه الأموال من أرباح أو فوائد أو ريع أو أي ناتج آخر، سواء بقيت على حالها أم تم تحويلها كليًا أو جزئيًا إلى ممتلكات أو عائدات استثمارية أخرى".

أما المقصود بالجريمة الأصلية هو "كل فعل يشكل جناية أو جنحة، وفقًا للتشريعات النافذة في الدولة، سواء ارتكب داخل الدولة أم خارجها، متى تولد عنه مال، وكان معاقبًا عليه في كلتا الدولتين"، وهذا يعني أن المشرع القطري اختط نهج التشريعات الجنائية التي لم تحصر حصول الأموال من جرائم بعينها بل، من أي جريمة، سواء كانت جناية أم جنحة، كالتشريع الفرنسي في المادة 324-1، والكويتي في المادة 1 من قانون مكافحة غسل الأموال رقم 35 لسنة 2002 والتونسي في المادة 1 من قانون رقم 75 لسنة 2003 والعماني في المادة 1 من القانون رقم 34 لسنة 2002 واللبناني في المادة 1 من القانون رقم 318 لسنة 2001، بينما اختطت تشريعات أخرى نهجًا مغايرًا عندما حددت جرائم معينة يتحصل منها الأموال، ومن هذه التشريعات التشريع المصري في المادة رقم 2 من القانون رقم 80 لسنة 2002 والسوري في المادة 1 الفقرة ج من القانون رقم 59 لسنة 2003، وكذلك سار على هذا النهج القانون الليبي والسوداني واليمني[16].

(16) جاسم، عمار باسل، جريمة غسل الأموال في القانون العراقي، عالم المعرفة للكتاب العراق 2011 ص50.

يستفاد من النص آنف الذكر أنه يشترط في الجريمة الأصلية أن تكون جناية أو جنحة طبقًا للقانون القطري، أما بالنسبة للجناية فإنه وطبقًا لنص المادة 22 من قانون العقوبات القطري يقصد بها "الجرائم المعاقب عليها بالإعدام أو الحبس المؤبد أو الحبس الذي يزيد عن ثلاث سنوات"، أما بالنسبة للجنحة فيقصد بها "الجرائم المعاقب عليها بالحبس لمدة لا تزيد على ثلاث سنوات وبالغرامة التي تزيد على ألف ريال أو بالتشغيل الاجتماعي".

إذا ثبت أن الأموال متحصلة عن جريمة وفقًا لما ذكر أعلاه، فإنه يستوي أن تكون الأموال، أصول أو ممتلكات أيًا كان نوعها، مادية أو غير مادية، ملموسة أو غير ملموسة، منقولة أو ثابتة، بما في ذلك الأصول المالية والموارد الاقتصادية كالنفط والموارد الطبيعية الأخرى وكافة الحقوق المتعلقة بها، أيًا كانت قيمتها وطريقة الحصول عليها، وجميع الوثائق أو المستندات القانونية أيًا كان شكلها بما في ذلك الصور الرقمية أو الإلكترونية، التي تثبت حق ملكية تلك الأصول، أو حصة فيها، وكذلك الأرباح أو الفوائد أو الريع أو أي مداخيل أخرى ناتجة عنها أو أي أصول أخرى يحتمل استخدامها للحصول عى تمويل أو سلع أو خدمات"[17].

الفرع الثاني: الركن المادي

يذهب جانب من الفقه[18] إلى أن جرائم غسل الأموال هي أقرب ما تكون إلى جرائم السلوك المجرّم؛ حيث عمد المشرع حال تحديده للواقعة محل التجريم إلى تجريم السلوك الإجرامي فقط وجعله مناطًا للعقاب، وبدورنا نتفق تمامًا مع من ذهب إلى هذا الاتجاه باعتبار جرائم غسل الأموال من جرائم الخطر وليس من جرائم الضرر التي تتطلب نتيجة إجرامية بل يكفي لقيام الجريمة ارتكاب السلوك المجرّم، سندنا في ذلك أحكام المادة 2 من قانون مكافحة غسل الأموال القطري رقم 20 لسنة 2019 حيث نصت على أنه "يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية: 4... أو الشروع في ارتكاب أي من الأفعال المحددة في هذه المادة يعد مرتكبًا لهذه الجريمة"، يستفاد من ذلك أن المشرع اعتبر الشروع جريمة تامة بنص خاص، وعاقب عليه بعقوبة الجريمة التامة وليس بمقتضى أحكام المادة 29 من قانون العقوبات التي تعاقب بعقوبة أخف من عقوبة مرتكب الجريمة التامة، وعليه لا يتصور الشروع في هذا النوع من الجرائم.

(17) المادة 1 من قانون مكافحة غسل الأموال وتمويل الإرهاب القطري رقم 20 لسنة 2019.

(18) النقرش، أمجد، البنيان القانوني لجريمة غسل الأموال، المجلة القانونية، العدد الخامس، البحرين، (2016) ص308.

أما من حيث صور التجريم وطبقًا لنص المادة آنفة الذكر فهي على النحو التالي:

الصورة الأولى: تحويل أو نقل الأموال غير المشروعة:

يقصد بتحويل الأموال طبقًا لتعليمات مصرف قطر المركزي بشأن مكافحة غسل الأموال وتمويل الإرهاب لسنة 2020 أنها تشير "إلى قبول النقد أو الشيكات أو غير ذلك من الأدوات النقدية أو مخازن القيم أو دفع مبلغ معادل نقدًا أو في أي صورة لمستفيد عن طريق اتصال أو رسالة أو تحويل أو عن طريق شبكة مقاصة تنتمي إليها هذه الخدمة المختصة بتحويل الأموال أو القيمة" بعبارة أخرى إن تحويل الأموال يتم عن طريق القنوات المصرفية أو المالية

أما نقل الأموال فيقصد بها انتقال الأموال من بلد إلى آخر، أي الأموال التي تهرب إلى الخارج بقصد المضاربة أو بسبب سوء الأحوال الاقتصادية والسياسية أو وجود أنظمة رقابية صارمة على التعامل بالنقد الأجنبي[19].

الصورة: الثانية: إخفاء أو تمويه الطبيعة الحقيقية للأموال غير المشروعة:

يقصد بالإخفاء كل عمل من شأنه منع كشف حقيقة المصدر غير المشروع وبأي شكل من الأشكال وبأي وسيلة، سواء كان هذا الإخفاء مستورًا أم علنيًا، فلا عبرة إذن بكون الإخفاء قد جرى سرًا، كما لا يهم وسيلة الإخفاء، فحتى لو تم بوسائل مشروعة كشراء الأموال المتحصلة عن الجريمة.

أما المقصود بالتمويه، فهو اصطناع مشروع غير حقيقي للأموال غير المشروعة، كإدخال الأموال القذرة في صلب الأرباح الناتجة عن إحدى الشركات المشروعة فتظهر هذه الأموال وكأنها أموال مشروعة[20].

تجدر الإشارة إلى أن المشرع القطري -وعلى غرار التشريعات المقارنة- لم يحدد أفعال السلوك في عملية الإخفاء أو التمويه، وبالتالي فإن المشرع يعتد بأي فعل أو امتناع عن فعل يؤدي إلى إخفاء أو تمويه حقيقة أو طبيعة الأموال غير المشروعة، وبذلك فإن هذه الجريمة تنتمي إلى الجرائم ذات القالب الحر[21]، ومع ذلك يجب إثبات السلوك الذي ترتب عليه إخفاء أو تمويه حقيقة الأموال غير المشروعة.

(19) الدليمي، الحديثي، مرجع سابق ص127.

(20) الحاجي، عمر غسيل الأموال، دار المكتبي، الطبعة الأولى، دمشق، (2005) ص72.

(21) الدليمي، الحديثي، المرجع السابق، ص128.

الصورة الثالثة: اكتساب أو حيازة أو استخدام الأموال غير المشروعة:

اعتبر المشرع القطري اكتساب أو حيازة أو استخدام الأموال غير المشروعة جريمة يعاقب عليها القانون، وهو بذلك – وخيرًا فعل – وسع من دائرة المساءلة الجنائية لتطال ليس فقط من حول أو نقل أو أخفى أو موه طبيعة الأموال غير المشروعة، بل وكذلك جرم من اكتسبها أي تملكها، حتى لو كان ذلك بمقتضى عقد قانوني كعقد البيع أو الهبة أو بشكل غير قانوني كسرقتها، أو أنه حازها بشكل قانوني بموجب عقد أمانة أو إيجار، أو بشكل غير قانوني كأن يضعها الجاني في الجريمة الأصلية التي تحصلت منها تلك الأموال بحيازة شخص آخر حتى يبعد الشبهات عنه، أو أن يكون الجاني قد قام باستخدام الأموال غير المشروعة كاستخدامه سيارة متحصلة عن جريمة.

الفرع الثالث: الركن المعنوي

ذهبت غالب التشريعات الجنائية المقارنة إلى اعتبار جرائم غسل الأموال من الجرائم العمدية، بينما ذهبت القلة منها إلى تصور وقوعها عن طريق الخطأ كالتشريعين السويسري والألماني[22]، وبالنسبة للفقه الجنائي فيذهب البعض إلى تبني تصور وقوع جرائم غسل الأموال عن طريق العمد، وكذلك الخطأ تعزيزًا وتوسيعًا لنطاق المسؤولية الجنائية عن هذه الجرائم، أما إذا سكت المشرع عن تحديد صورة الركن المعنوي في جرائم غسل الأموال وعندها نطبق القاعد القاضية بأن الأصل في التجريم العمد.[23]

بالنسبة لموقف المشرع القطري فقد حسم موقفه بهذا الشأن فاعتبر جرائم غسل الأموال من الجرائم العمدية بصريح نص المادة 2 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019، حيث نص المشرع على أنه "يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية..."، وبالتالي لا يمكن تصور وقوع الجريمة عن طريق الخطأ.

وبهذا المعنى، فإنه يشترط لقيام جريمة غسل أموال، توفر القصد الجنائي العام، لكن يثور التساؤل هل نحن بحاجة إلى القصد الجنائي الخاص، أم نكتفي بالقصد الجنائي العام؟

عند مراجعة نص المادة 2 آنفة الذكر نجد أن المشرع طلب قصدًا جنائيًا خاصًا في صورة تحويل أو نقل الأموال، أما في صورة الإخفاء أو التمويه أو في صورة الاكتساب أو الحيازة أو الاستخدام فقد اكتفى المشرع بالقصد الجنائي العام، وذلك على النحو التالي:

(22) الفقرة الثالثة من المادة 305 مكرر من قانون العقوبات السويسري، والفقرة الخامسة من المادة 261 من قانون مكافحة الجريمة المنظمة الألماني

(23) انظر في ذلك الدليمي والحديثي، المرجع السابق، ص166.

أما في صورة تحويل أو نقل الأموال، فالقصد الجنائي العام يتمثل فيها بعلم الجاني أن فعله يترتب عليه نقل أو تحويل أموال، وأن يعلم أن هذه الأموال متحصلة عن جريمة، ويريد فعله، أما القصد الجنائي الخاص في هذه الصورة فيتمثل اتجاه إرادته إلى إخفاء أو تمويه المصدر غير المشروع لتلك الأموال.

أما في صورة الإخفاء أو التمويه، فنكتفي فقط بالقصد الجنائي العام، والمتمثل بعلم الجاني أن فعله يترتب عليه إخفاء أو تمويه حقيقة أموال، وأن يعلم أن هذه الأموال متحصلة عن جريمة، وأن تتجه إرادته إلى الإخفاء أو التمويه.

أما في صورة الاكتساب أو الحيازة أو الاستخدام، فكذلك الحال في الصورة السابقة لا نحتاج أكثر من القصد الجنائي العام والمتمثل هنا بعلم الجاني أنه يكتسب أو يحوز أو يستخدم أموالاً، وأن يعلم أن هذه الأموال متحصلة عن جريمة، وأن تتجه إرادته إلى ذلك الاكتساب أو الحيازة أو الاستخدام.

أما من حيث إثبات القصد الجنائي في هذه الجريمة فإنه "يجوز الاستدلال على العلم والإرادة اللازمين لإثبات جريمة غسل الأموال أو جريمة تمويل الإرهاب من الظروف الواقعية الموضوعية"[24].

الفرع الرابع: عقوبة جريمة غسل الأموال

تعددت العقوبات التي قررتها الاتفاقيات الدولية والتشريعات الوطنية لدول مختلفة بالنسبة لجرائم غسل الأموال، ويحكم تلك العقوبات اتجاه سائد وهو تقرير عقوبات ذات طبيعة مختلفة، فمنها العقوبات السالبة للحرية والعقوبات المالية، ومنها كذلك التدابير الاحترازية[25]، ولا يتسع المقام لاستعراضها لا سيما أن موضوع البحث يركز على خروج جرائم غسل الأموال عن الأحكام العامة، ومنها تلك الأحكام العامة المتعلقة بعقوبة الشخص الاعتباري وهو ما سوف نتناوله لاحقًا في مطلب مستقل.

قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة القطري،2019 تضمن عقوبات للشخص الطبيعي وكذلك الشخص المعنوي عند ارتكاب إحدى صور غسل الأموال الواردة فيه، وذلك على النحو التالي:

(24) المادة 5 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019.

(25) عبدالله، مازن نجم، جريمة غسيل الأموال في التشريع العراقي، منشورات المكتبة القانونية، بغداد العراق ص72.

أولًا: عقوبات الشخص الطبيعي:

إذا ارتكب الشخص الطبيعي أي جريمة من جرائم غسل الأموال الواردة في المادة 2 من ذات القانون، فإن عقوبة ذلك هي الحبس لمدة لا تجاوز عشر سنوات والغرامة التي لا تقل عن مليوني ريال ولا تزيد على خمسة ملايين ريال، أو ضعف قيمة الأموال التي تم غسلها أيهما أكثر[26]، وتضاعف العقوبة المذكورة آنفًا في حالة العود أو إذا ارتكبت من قبل مجموعة من الأشخاص يعملون لهدف مشترك أو وقعت من شخص استغل سلطته أو نفوذه[27] كذلك توقع عقوبة مصادرة الأموال التي تشكل موضوع الجريمة أو الأموال المتحصلة عن الجريمة، أو الأموال التي تشكل إيرادات ومنافع أخرى متأتية من تلك الأموال أو من متحصلات الجريمة[28]، هذا وفي حالة تعدد الجناة فإنه يعفى مرتكب جريمة غسل الأموال من العقوبة إذا بادر إلى إبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن

(26) المادة 78 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019، حيث نصت على أنه "يعاقب بالحبس لمدة لا تجاوز عشر سنوات، وبالغرامة التي لا تقل عن (2,000,000) مليوني ريال ولا تزيد على (5,000,000) خمسة ملايين ريال، أو ضعف قيمة الأموال التي تم غسلها , أيهما أكثر، كل من ارتكب إحدى جرائم غسل الأموال، المنصوص عليها في المادة (2) من هذا القانون"

(27) المادة 88 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019.

تضاعف العقوبات المنصوص عليها في المادتين (78) و (79) من هذا القانون على النحو التالي:

- في حال العود، ويعتبر المتهم عائدًا إذا ارتكب جريمة مماثلة خلال خمس سنوات من تاريخ انتهاء تنفيذ العقوبة المحكوم بها أو سقوطها بمضي المدة
- في حال المساهمة أو الشروع في ارتكاب جريمة واحدة أو أكثر من جرائم غسل الأموال أو تمويل الإرهاب، وذلك من قبل مجموعة من الأشخاص يعملون بهدف مشترك
- في حال ارتكاب الجريمة من شخص مستغل لسلطاته أو نفوذه في مؤسسة مالية أو أي من الأعمال والمهن غير المالية المحددة أو مستغلًا للصلاحيات التي خولتها له وظيفته أو نشاطه المهني أو الاجتماعي

(28) المادة 89 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019.

في حالة الإدانة بارتكاب جريمة غسل الأموال أو جريمة أصلية أو تمويل الإرهاب , ومع عدم الإخلال بحقوق الغير حسن النية، تقضي المحكمة بمصادرة ما يلي

- الأموال التي تشكل موضوع الجريمة.
- الأموال التي تشكل متحصلات جريمة، بما في ذلك الأموال المختلطة بتلك المتحصلات أو المتأتية منها أو المبدلة بها، أو أموال تعادل قيمتها قيمة تلك المتحصلات
- الأموال التي تشكل إيرادات ومنافع أخرى متأتية من تلك الأموال أو من متحصلات الجريمة.
- وسائط ارتكاب الجريمة.

ويكون الغير حسن النية إذا تحصل على الأموال المشار إليها أو جزء منها أو اكتسبها وكان يجهل مصدرها غير المشروع أو مقابل دفع ثمن أو تقديم خدمات مناسبة لقيمتها أو بناءً على أسباب مشروعة أخرى

وفي حالة وقوع جريمة معاقب عليها بموجب أحكام هذا القانون، عدم إدانة فاعلها لعدم معرفته أو لوفاته، يجوز للنيابة العامة أن ترفع الأوراق للمحكمة المختصة، لإصدار حكم بمصادرة الأموال المحجوزة، إذا قدمت أدلة كافية تثبت أنها من متحصلات الجريمة. وفي جميع الأحوال , يتعين أن يحدد حكم المصادرة الأموال المعنية، وأن يتضمن التفاصيل اللازمة لتحديدها وتعيين موقعها

الأشخاص المشتركين فيها، وذلك قبل علمها بها أو قبل البدء في تنفيذها، أما إذا حصل الإبلاغ بعد علم الجهات المختصة بالجريمة، وبالأشخاص المشتركين فيها، وأدى إلى ضبط باقي الجناة أو وسائط ومتحصلات الجريمة فإنه يجوز للمحكمة في هذه الحالة أن تحكم بوقف تنفيذ العقوبة، غير أن ذلك لا يشمل عقوبة المصادرة التي يجب تنفيذها في كل الأحوال[29].

ثانيًا: عقوبات الشخص المعنوي (الاعتباري):

إذا ارتكب شخص طبيعي يعمل منفردًا أو كجزء من جهاز تابع للشخص المعنوي، أو يشغل موقعًا قياديًا فيه أو يستند إلى تمثيله، أو لديه تفويض باتخاذ القرار نيابة عنه، أو مخول بممارسة السلطة فيه، جريمة غسل الأموال باسم ولصالح الشخص المعنوي فإن الأخير توقع عليه عقوبة الغرامة التي لا تقل عن أربعة ملايين ريال ولا تزيد عن ثمانية ملايين ريال، أو ثلاثة أضعاف الحد الأقصى للغرامة المقررة للجريمة أيهما أكثر، كذلك للمحكمة أن تفرض عليه عقوبة المنع من مزاولة أي نشاط من أنشطته سواء بصورة مؤقتة أو دائمة، أو بوضعه تحت إشراف قضائي، كذلك يجوز للمحكمة الحكم بإغلاقه بشكل مؤقت أو دائم، ولها أيضًا الحكم بحله وتصفيته، وأخيرًا لها أن تحكم بنشر الحكم في جريدتين رسميتين على نفقة الشخص المعنوي.[30]

المطلب الثاني: موقف اتفاقية الأمم المتحدة لمكافحة الفساد من جرائم غسل الأموال

نخصص هذا المطلب لاستعراض موقف اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003 بشأن ضرورة مواءمة التشريعات الجنائية الوطنية معها لتجريم هذا النوع من الجرائم.

---

(29) المادة 92 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019حيث نصت على أنه (في حالة تعدد الجناة، يعفى مرتكب جريمة غسل الأموال أو تمويل الإرهاب من العقوبة المنصوص عليها في هذا القانون إذا بادر إلى إبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علمها بها أو قبل البدء في تنفيذها. ويجوز للمحكمة أن تحكم بوقف تنفيذ العقوبة، إذا حصل الإبلاغ بعد علم الجهات المختصة بالجريمة، وبالأشخاص المشتركين فيها، وأدى إلى ضبط باقي الجناة أو وسائط ومتحصلات الجريمة. ولا يحول الإعفاء أو إيقاف تنفيذ العقوبة من مصادرة متحصلات الجريمة أو وسائطها

(30) المادة 77 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019 حيث نصت على أنه "يعاقب بالغرامة التي لا تقل عن (4,000,000) أربعة ملايين ريال ولا تزيد على (8,000,000) ثمانية ملايين ريال، أو ثلاثة أضعاف الحد الأقصى للغرامة المقررة للجريمة، أيهما أكثر، كل شخص معنوي، ارتُكبت إحدى الجرائم المنصوص عليها في هذا القانون باسمه ولصالحه من جانب شخص طبيعي يعمل منفردًا أو كجزء من جهاز تابع له، أو يشغل موقعًا قياديًا فيه أو يستند إلى تمثيله، أو لديه تفويض باتخاذ القرار نيابة عنه، أو مخول بممارسة السلطة فيه .ولا يحول ذلك دون معاقبة الشخص الطبيعي مرتكب الجريمة، بالعقوبة المقررة لها في هذا القانون. وللمحكمة أن تقضي بمنع الشخص المعنوي، من مواصلة القيام بأنشطة تجارية معينة بصورة مباشرة أو غير مباشرة وبشكل دائم أو مؤقت أو بوضعه تحت إشراف قضائي أو بإغلاق مرافقه التي استخدمت في ارتكاب الجريمة بصفةٍ دائمة أو مؤقتة أو بحله وتصفية أعماله. ولها أن تأمر بنشر الحكم الصادر ضده على نفقته الخاصة في جريدتين يوميتين"

لقد أفردت اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003، مادتين بهذا الشأن، حيث نظمت المادة 14 منها التدابير الوقائية المطلوب اتخاذها من قبل الدول الأطراف فيها، ومنها، على كل دولة طرف إنشاء نظام داخلي للرقابة والإشراف على المصارف أو المؤسسات المالية غير المصرفية، وأن تمكن سلطاتها الإدارية والرقابية المعنية بإنفاذ القانون وكافة السلطات المكرسة لمكافحة الفساد من التعاون وتبادل المعلومات على الصعيدين الوطني والدولي، وأن تقوم بإنشاء وحدة معلومات مالية تعمل كمركز وطني لجمع وتحليل المعلومات المتعلقة بعمليات غسل الأموال المحتملة وتعميم تلك المعلومات، كذلك اتخاذ تدابير رقابة حركة النقود والصكوك عبر حدودها، وكذلك على الدول الأطراف إلزام مؤسساتها المالية، وعلى وجه الخصوص تلك المختصة بالتحويلات المالية، أن تنظم استمارة إلكترونية لأي عملية تحويل أموال تبين مصدر تلك الأموال، والاحتفاظ بتلك المعلومات وفحصها وتدقيقها، كذلك على الدول الأطراف فيما يتعلق بشأن الرقابة على حركة الأموال، أن تسترشد بالمعايير الدولية بهذا الشأن، أخيرًا فإن الاتفاقية الأممية دعت الدول الأطراف إلى تنمية وتعزيز التعاون العالمي والإقليمي ودون الإقليمي والثنائي بين السلطات القضائية وأجهزة إنفاذ القانون وأجهزة الرقابة المالية من أجل مكافحة غسل الأموال.[31]

(31) للتفصيل انظر المادة 14 من اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003 حيث نصت على "تدابير منع غسل الأموال -1 على كل دولة طرف

(أ) أن تنشئ نظامًا داخليًّا شاملًا للرقابة والإشراف على المصارف والمؤسسات المالية غير المصرفية، بما في ذلك الشخصيات الطبيعية أو الاعتبارية التي تقدم خدمات نظامية أو غير نظامية في مجال إحالة الأموال أو كل ما له قيمة، وعند الاقتضاء على الهيئات الأخرى المعرّضة بوجه خاص لغسل الأموال، ضمن نطاق اختصاصها، من أجل ردع وكشف جميع أشكال غسل الأموال، ويتعين أن يشدد ذلك النظام على المتطلبات الخاصة بتحديد هوية الزبائن والمالكين المنتفعين، عند الاقتضاء، وحفظ السجلات والإبلاغ عن المعاملات المشبوهة؛ (ب) أن تكفل، دون مساس بأحكام المادة 46 من هذه الاتفاقية، قدرة السلطات الإدارية والرقابية والمعنية بإنفاذ القانون وسائر السلطات المكرسة لمكافحة غسل الأموال، (بما فيها السلطات القضائية، حيثما يقضي القانون الداخلي بذلك)، على التعاون وتبادل المعلومات على الصعيدين الوطني والدولي ضمن نطاق الشروط التي يفرضها قانونها الداخلي، وأن تنظر، لتلك الغاية، في إنشاء وحدة معلومات استخبارية مالية تعمل كمركز وطني لجمع وتحليل المعلومات المتعلقة بعمليات غسل الأموال المحتملة، ولتعميم تلك المعلومات؛ -2 تنظر الدول الأطراف في تنفيذ تدابير قابلة للتطبيق لكشف ورصد حركة النقود والصكوك القابلة للتداول ذات الصلة عبر حدودها، رهنا بضمانات تكفل استخدام المعلومات استخدامًا سليمًا ودون إعاقة حركة رأس المال المشروع بأي صورة من الصور. ويجوز أن تشمل تلك التدابير اشتراط قيام الأفراد والمؤسسات التجارية بالإبلاغ عن إحالة أي مقادير ضخمة من النقود والصكوك القابلة للتداول ذات الصلة عبر الحدود. -3 تنظر الدول الأطراف في تنفيذ تدابير مناسبة وقابلة للتطبيق لإلزام المؤسسات المالية، ومنها الجهات المعنية بتحويل الأموال بما يلي: (أ) تضمين استمارات الإحالة الإلكترونية للأموال والرسائل ذات الصلة معلومات دقيقة ومفيدة عن المُصدر؛ (ب) الاحتفاظ بتلك المعلومات طوال سلسلة عمليات الدفع؛ (ج) فرض فحص دقيق على إحالات الأموال التي لا تحتوي على معلومات كاملة عن المُصدر. -4 لدى إنشاء نظام رقابي وإشرافي داخلي بمقتضى أحكام هذه المادة، ودون مساس بأي مادة أخرى من هذه الاتفاقية، يجدر بالدول الأطراف أن تسترشد بالمبادرات ذات الصلة التي اتخذتها المؤسسات الإقليمية والأقاليمية والمتعددة الأطراف ضد غسل الأموال. -5 تسعى الدول الأطراف إلى تنمية وتعزيز التعاون العالمي والإقليمي ودون الإقليمي والثنائي بين السلطات القضائية وأجهزة إنفاذ القانون وأجهزة الرقابة المالية من أجل مكافحة غسل الأموال

أما المادة 23 من ذات الاتفاقية، فقد ألزمت الدول الأطراف باتخاذ التدابير التشريعية اللازمة لتجريم عمليات غسل الأموال إذا لم تكن مجرمة بموجب قانونها الداخلي، وقد رسمت الملامح الرئيسية لنموذج التجريم الواجب إقراره، ومن هذه الملامح أن جريمة غسل الأموال هي من الجرائم العمدية التي لا تقع عن طريق الخطأ، وأن من صورها إبدال الممتلكات أو إحالتها مع العلم أنها متحصلة عن جريمة، أو إخفاء تلك الأموال أو التمويه عليها بقصد إخفاء المصدر غير المشروع لتلك الأموال، ويشمل التجريم امتلاكها أو حيازتها أو التعامل بها بأي شكل من الأشكال، كذلك تجريم المشاركة أو الشروع في هذه الجرائم.[32]

المبحث الثالث
حالات خروج جرائم غسل الأموال عن الأحكام العامة

تضمن قانون مكافحة جرائم غسل الأموال وتمويل الإرهاب القطري رقم 20 لسنة 2019 أحكامًا مثلت خروجًا عن القواعد العامة اقتضتها طبيعة وخطورة هذه الجريمة، سواء من حيث أحكام الاشتراك أو الشروع أو الارتباط أم من حيث سريان قانون العقوبات من حيث المكان أو عقوبة الشخص المعنوي.

(32) للتفصيل انظر نص المادة 23من اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003 حيث نصت على أنه "-1 تعتمد كل دولة طرف، وفقًا للمبادئ الأساسية لقانونها الداخلي، ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية، عندما ترتكب عمدًا: (أ) "1" إبدال الممتلكات أو إحالتها، مع العلم بأنها عائدات إجرامية، بغرض إخفاء أو تمويه مصدر تلك الممتلكات غير المشروع أو مساعدة أي شخص ضالع في ارتكاب الجرم الأصلي على الإفلات من العواقب القانونية لفعلته؛ "2" إخفاء أو تمويه الطبيعة الحقيقية للممتلكات أو مصدرها أو مكانها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، مع العلم بأن تلك الممتلكات هي عائدات إجرامية؛(ب) ورهنًا بالمفاهيم الأساسية لنظامها القانوني '1' اكتساب الممتلكات أو حيازتها أو استخدامها مع العلم، وقت استلامها، بأنها عائدات إجرامية؛ '2' المشاركة في ارتكاب أي فعل مجرّم وفقًا لهذه المادة، أو التعاون أو التآمر على ارتكابه، والشروع في ارتكابه والمساعدة والتشجيع على ذلك وتسهيله وإسداء المشورة بشأنه. -2 لأغراض تنفيذ أو تطبيق الفقرة 1 من هذه المادة: (أ) تسعى كل دولة طرف إلى تطبيق الفقرة 1 من هذه المادة على أوسع مجموعة من الجرائم الأصلية؛ (ب) تدرج كل دولة طرف في عداد الجرائم الأصلية، كحد أدنى، مجموعة شاملة من الأفعال المجرّمة وفقًا لهذه الاتفاقية؛ (ج) لأغراض الفقرة الفرعية (ب) أعلاه، تشمل الجرائم الأصلية الجرائم المرتكبة داخل الولاية القضائية للدولة الطرف المعنية وخارجها. غير أن الجرائم المرتكبة خارج الولاية القضائية للدولة الطرف لا تمثل جرائم أصلية إلا إذا كان السلوك ذا الصلة يعتبر فعلًا إجراميًّا بمقتضى القانون الداخلي للدولة التي ارتكب فيها وكان من شأنه أن يعتبر فعلًا إجراميًّا بمقتضى القانون الداخلي للدولة الطرف التي تُنفِّذ أو تُطبّق هذه المادة لو كان قد ارتكب هناك؛(د) تزوّد كل دولة طرف الأمين العام للأمم المتحدة بنسخ من قوانينها المُنْفذة لهذه المادة وبنسخ من أي تغييرات تُدخل على تلك القوانين لاحقًا أو بوصف لها؛ (هـ) يجوز النص على أن الجرائم المبيّنة في الفقرة 1 من هذه المادة لا تسري على الأشخاص الذين ارتكبوا الجرم الأصلي إذا كانت المبادئ الأساسية للقانون الداخلي للدولة الطرف تقتضي بذلك

تقسيم

نتناول في هذا المبحث أوجه خروج جرائم غسل الأموال عن الأحكام العامة، حيث نبحث في المطلب الأول خروجها عن الأحكام العامة للاشتراك الجرمي، وفي المطلب الثاني خروجها عن أحكام الشروع، وفي الثالث خروجها عن أحكام الارتباط بين الجرائم، وفي الرابع خروجها عن أحكام سريان القانون من حيث المكان، وفي الخامس خروجها من حيث عقوبة الشخص المعنوي، أما المطلب السادس فقد أفردناه لبحث اقتراح تضمين قانون مكافحة غسل الأموال القطري النافذ، حكم استثنائي يتعلق باستبعاد التقادم الجنائي في هذا النوع من الجرائم.

المطلب الأول: من حيث أحكام الاشتراك

طبقًا للأحكام العامة في قانون العقوبات القطري وتحديدًا المادة (39)، فإن صور الاشتراك الجرمي أو ما يطلق عليه المساهمة التبعية تقع بإحدى الصور الثلاث، إما بالتحريض أو المساعدة أو الاتفاق، غير أن المادة 2 من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019 قد خرجت عن هذا الأصل، فعدت من يشارك أو يساهم بأي صورة من صور التجريم الواردة بذات المادة فاعلاً أصليًا في الجريمة وليس شريكًا، حيث نصت على أنه "يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية: .....4- الاشتراك أو الارتباط أو التواطؤ أو المساعدة أو التحريض أو التسهيل أو تقديم المشورة أو التعاون أو المساهمة أو التآمر في ارتكاب أو الشروع في ارتكاب أي من الأفعال المحددة في هذه المادة" أي إن الصور آنفة الذكر من حيث الأصل ما هي إلا صور للاشتراك الجرمي، بيد أن المشرع القطري خرج عن الأحكام العامة واعتبرها أفعالاً أصلية.

تجدر الإشارة إلى أن النص آنف الذكر يؤخذ عليه أنه عدد صور ما كان بحاجة إلى تعدادها أو ذكرها وكان الأفضل ذكر مصطلح الاشتراك فقط، دون الحاجة إلى ذكر المساعدة أو التسهيل أو تقديم المشورة أو التعاون أو المساهمة، فكلها تدخل ضمن مفهوم أعمال الاشتراك.

أخيرًا، قد يثور تساؤل حول جدوى التفريق بين الفاعل وبين الشريك طالما أن المشرع القطري قد ساوى في العقاب بينهما طبقًا لنص المادة (40) من قانون العقوبات، حيث نصت على أنَّ (من اشترك في جريمة عوقب بعقوباتها ما لم ينص القانون على خلاف ذلك) الإجابة على هذا التساؤل هو أن هناك أهمية للتفريق بينهما من الناحية القانونية ومن الناحية العملية، أما من الناحية القانونية فإن القانون أحيانًا يتطلب صفة معينة في

الفاعل دون الشريك يترتب عليها تغير الوصف الجرمي، كتطلب القانون صفة الموظف العام للفاعل في جريمة الرشوة دون الشريك (الراشي أو الوسيط)، أما من الناحية العملية فإن المحكمة غالبًا ما تحكم بعقوبة أشد من تلك التي تعاقب بها الشريك إعمالاً لسطلتها التقديرية في العقاب بين الحد الأقصى والأدنى.[33]

المطلب الثاني: من حيث أحكام الشروع

طبقًا لأحكام المادة 39 من قانون مكافحة غسل الأموال وتمويل الإرهاب القطري رقم 20 لسنة 2019 اعتبر المشرع القطري الشروع بأي صورة من صور التجريم الواردة بذات المادة آنفة الذكر جريمة تامة، وليس شروعًا فيها، حيث نصت على أنه "يُعد مرتكبًا لجريمة غسل الأموال كل من قام عمدًا بأي من الأفعال التالية: .....4- الاشتراك أو الارتباط أو التواطؤ أو المساعدة أو التحريض أو التسهيل أو تقديم المشورة أو التعاون أو المساهمة أو التآمر في ارتكاب أو الشروع في ارتكاب أي من الأفعال المحددة في هذه المادة"، وبالتالي يعاقب بعقوبة الجريمة التامة، وهذا التشدد المبرر من جانب المشرع القطري إنما تقتضيه خطورة هذه الجريمة.

تجدر الإشارة في هذا المقام إلى أن عقوبة الشروع تكون أخف من عقوبة الجريمة الأصلية، ولهذا عمد المشرع إلى اعتبار أفعال الشروع باعتبارها أفعالاً تامة بغية أن ينال الجاني في هذا النوع من الجرائم أقصى درجات العقاب.

المطلب الثالث: من حيث ارتباط جريمة غسل الأموال بالجريمة الأصلية

على الرغم من أن أحد أركان جريمة غسل الأموال هو أن يكون محلها أموالاً متحصلة عن جريمة، بعبارة أخرى، أن هناك ارتباطًا بين الجريمة الأصلية وجريمة غسل الأموال باعتبار الأموال المتحصلة عن الجريمة الأصلية أحد أركان جريمة غسل الأموال، إلا أنه وبالرغم من هذا الارتباط فإن المشرع القطري قرر استقلالهما عن بعض، حيث نصت الفقرة الأخيرة من المادة 2 آنفة الذكر على أنه "وتعتبر جريمة غسل الأموال جريمة مستقلة عن الجريمة الأصلية.." وهو أيضًا ما أكدت عليه المادة 76 من القانون ذاته بقولها "لا تخضع جرائم غسل الأموال وتمويل الإرهاب لأحكام المادة (85) من قانون العقوبات المشار إليه".

(33) غنام، غنام محمد شرح قانون العقوبات القطري الأحكام العامة، الطبعة الأولى، منشورات كلية القانون –جامعة قطر، (2017) ص236.

جدير بالذكر أن المادة 85 من قانون العقوبات القطري نصت على أنه "إذا وقعت عدة جرائم لغرض واحد وكانت مترابطة ببعضها ارتباطًا لا يقبل التجزئة فيجب اعتبارها كلها جريمة واحدة والحكم بالعقوبة الأشد المقررة لأي من تلك الجرائم"، يستفاد من ذلك أن نص المادة 85 لا ينطبق على جرائم غسل الأموال؛ إذ تعتبر الجريمة الأصلية مستقلة عن جريمة غسل الأموال، فإذا كان الجاني هو ذاته الذي ارتكب الجريمة الأصلية التي تحصل منها على الأموال غير المشروعة، وكذلك ارتكب جريمة غسل الأموال، فإنه يحكم عليه بعقوبة الجريمة الأصلية وبعقوبة جريمة غسل الأموال بكل الأحوال ودون اعتبار لأيهما أشد أو أخف فيتم الحكم بعقوبة الجريمة الأصلية وعقوبة جريمة غسل الأموال إعمالاً لحكم النص، وهذا ما أكدته المادة 2 من القانون ذاته بقولها "... ولا تحول معاقبة الأشخاص الذين يرتكبون الجريمة الأصلية دون معاقبتهم على جريمة غسل الأموال".

المطلب الرابع: من حيث سريان قانون العقوبات

استنادًا إلى نص المادة 94[34] من قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019، يسري على جريمة غسل الأموال هذا القانون وإن ارتكبت خارج إقليم الدولة، وهذا خروج عن مبدأ الإقليمية المقرر في قانون العقوبات بموجب المادة 13 من قانون العقوبات القطري والذي يقضي بسريان قانون العقوبات على الجرائم التي ترتكب في دولة قطر، سواء وقع فعل من الأفعال المكونة لها أم إذا تحققت فيها نتيجتها، أم كان يراد أن تتحقق فيها.

يستفاد من حكم المادة 94 المذكورة آنفًا أن المشرع القطري أراد أن يشمل جرائم غسل الأموال بمبدأ عالمية النص الجنائي من خلال نص خاص أضاف من خلاله جريمة أخرى إلى الجرائم المشمولة بمبدأ العالمية الوارد في المادة 17 من قانون العقوبات القطري وهي جرائم الاتجار بالمخدرات أو الاتجار بالأشخاص أو جرائم القرصنة أو جرائم الإرهاب الدولي، نخلص إلى القول بأن القانون القطري يسري على أي جريمة من جرائم غسل الأموال الواردة في القانون إذا ارتكبها الجاني بوصفه فاعلاً أو شريكًا في الجريمة بشرط

(34) نصت المادة 94 من قانون رقم 20 لسنة 2019 بشأن مكافحة غسل الأموال وتمويل الإرهاب على أنه "مع مراعاة أحكام الاختصاص الواردة في قانون العقوبات المشار إليه، تسري أحكام هذا القانون في الحالات التالية
• إذا كانت الجريمة موجهة ضد مرفق حكومي أوعام تابع للدولة وموجود خارج إقليمها بما في ذلك الأماكن الدبلوماسية أوالقنصلية.
• إذا ارتكبت الجريمة في الخارج من شخص عديم الجنسية له محل إقامة معتاد في الدولة.
• كل من وجد في الدولة بعد أن ارتكب في الخارج , بوصفه فاعلًا أو شريكًا، أيًا من الجرائم المنصوص عليها في هذا القانون.
وتختص النيابة العامة بالتحقيق والاتهام ومباشرة الدعوى في الجرائم المنصوص عليها في الفقرة السابقة، كما تباشر محاكم الدولة اختصاصها على هذه الجرائم"

أن يكون الجاني متواجدًا في الدولة، وهذا الحكم يدخل ضمن إطار التعاون الدولي الرامي إلى مكافحة الجرائم التي تمس المجتمع الدولي برمته، وهنا نقترح على المشرع القطري إعادة النظر في المادة 17 من قانون العقوبات القطري لإدخال جريمة غسل الأموال ضمن الجرائم المشمولة بعالمية النص الجنائي.

المطلب الخامس: من حيث عقوبة الشخص المعنوي

طبقًا للقواعد العامة الواردة في القسم العام من قانون العقوبات القطري رقم 11 لسنة 2004 فإن المسؤولية الجنائية وعقوبة الشخص المعنوي قد وردت تحديدًا في المادة 37، حيث نصت على أنه (فيما عدا الوزارات والأجهزة الحكومية الأخرى والهيئات والمؤسسات العامة، يكون الشخص الاعتباري مسؤولاً جنائيًا عن الجرائم التي يرتكبها ممثلوه أو مديروه أو وكلاؤه لحسابه أو باسمه، ولا يجوز الحكم عليه بغير الغرامة، وما يتناسب من العقوبات الفرعية المقررة قانونًا، فإذا كان القانون يقرر للجريمة عقوبة أصلية غير الغرامة، اقتصرت العقوبة على الغرامة التي لا يزيد حدها الأقصى على خمسمائة ألف ريال، ولا يمنع ذلك من معاقبة مرتكب الجريمة شخصيًا بالعقوبة المقررة لها في القانون).

قبل تحديد وجه خروج جرائم غسل الأموال عن القواعد العامة آنفة الذكر، تجب الإشارة إلى أننا نتفق مع ما ذهب إليه بعض الشراح[35] من انتقاد نص المادة 37 من قانون العقوبات القطري، وعليه نسجل ملاحظة دستورية تتمثل في منح القاضي الجنائي "اختيار ما يتناسب من العقوبات الفرعية المقررة قانونًا" وبذلك أخذ القاضي دور المشرع في تحديد ما يتناسب من العقوبات المقررة للجريمة وهو ما يتعارض ويصطدم مع مبدأ الشرعية الجنائية الذي كفله الدستور القطري في المادة 40 حيث نص على أنه "لا جريمة ولا عقوبة إلا بقانون". بعبارة أخرى فإن مبدأ الشرعية أوجب أن يحدد القانون العقوبة على وجه الدقة ويترك للقاضي سلطة تقديرية للحكم بين الحد الأعلى والحد الأدنى، لا أن يترك للقاضي سلطة اختيار عقوبات لم يتضمنها نص التجريم، وعليه نقترح على المشرع القطري إعادة النظر في فقرة "اختيار ما يتناسب من العقوبات الفرعية المقررة قانونًا" لاستشكالها مع مبدأ الشرعية الجنائية، عودًا إلى موضوع عقوبة الشخص المعنوي على جرائم غسل الأموال في القانون القطري فإن المادة 77 من قانون مكافحة غسل الأموال وتمويل الإرهاب النافذ تضمنت حكمًا خاصًا بشأن عقوبة الشخص المعنوي، حيث قررت عقوبة الغرامة التي لا تقل عن أربعة ملايين ولا تزيد على ثمانية ملايين ريال، أو ثلاثة

(35) شمس الدين، أشرف ، شرح قانون العقوبات القطري –القسم العام، منشورات جامعة قطر-كلية القانون، الطبعة الأولى (2010) ص366.

أضعاف الحد الأقصى للغرامة المقررة للجريمة أيهما أكثر،[36] وبذلك نلاحظ اختلاف جرائم غسل الأموال بشأن عقوبة الشخص المعنوي عن الحد الأقصى للغرامة المقرر طبقًا للقواعد العامة الواردة في المادة 37 من قانون العقوبات القطري، وبذلك يعتبر نص المادة 77 من قانون غسل الأموال نصًا خاصًا يقيد النص العام الوارد في قانون العقوبات.

المطلب السادس: من حيث التقادم

ابتداءً يجب لفت الانتباه إلى أن المشرع القطري لم يخرج في جرائم غسل الأموال عن الأحكام العامة للتقادم الجنائي، بيد أننا أفردنا هذا المطلب لمطالبة المشرع القطري بضرورة التدخل التشريعي لاستبعاد أحكام التقادم الجنائي من التطبيق على جرائم غسل الأموال؛ كونها من أبرز جرائم الفساد، والتي دعت اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003 الدول الأطراف إلى استبعاد التقادم أو إطالة مدة التقادم في جرائم الفساد، حيث نصت المادة 29 من الاتفاقية ذاتها على أنه "تحدد كل دولة طرف في إطار قانونها الداخلي عند الاقتضاء، فترة تقادم طويلة تبدأ فيها الإجراءات القضائية بشأن أي فعل مجرم وفقًا لهذه الاتفاقية، وتحدد فترة تقادم أطول أو تعلق العمل بالتقادم في حال إفلات الجاني المزعوم من يد العدالة". غني عن البيان أن دولة قطر صادقت على الاتفاقية الأممية لمكافحة الفساد سنة 2007 وأصبحت جزءًا من التشريع الداخلي، وتجب المواءمة بينها وبين التشريعات الوطنية، ومن أوجه هذه المواءمة أن يتم استبعاد التقادم أو إطالة مدة التقادم في جرائم الفساد على أقل تقدير، ومنها بطبيعة الحال جرائم غسل الأموال موضوع البحث.

تجدر الإشارة إلى أن العديد من الأنظمة القانونية المقارنة لم تأخذ بمبدأ التقادم الجنائي في أحكامها العامة، ومنها القانون الإنجليزي والقانون العراقي والقانون السوداني وغيرها من القوانين، وعليه نقترح على المشرع القطري على أقل تقدير أن يعيد النظر في تطبيق التقادم الجنائي في جرائم غسل الأموال وتمويل الإرهاب.

(36) المادة 77 من قانون مكافحة غسل الأموال وتمويل الإرهاب القطري رقم 20 لسنة 2019 حيث نصت على أنه (إذا ارتكب شخص طبيعي يعمل منفردًا أو كجزء من جهاز تابع للشخص المعنوي، أو يشغل موقعًا قياديًا فيه أو يستند إلى تمثيله، أو لديه تفويض باتخاذ القرار نيابة عنه، أو مخول بممارسة السلطة فيه، جريمة غسل الأموال، باسم ولصالح الشخص المعنوي فإن الأخير توقّع عليه عقوبة الغرامة التي لا تقل عن أربعة ملايين ريال ولا تزيد على ثمانية ملايين ريال، أو ثلاثة أضعاف الحد الأقصى للغرامة المقررة للجريمة أيهما أكثر، كذلك للمحكمة أن تفرض عليه عقوبة المنع من مزاولة أي نشاط من أنشطته سواء بصورة مؤقتة أم دائمة، أم بوضعه تحت إشراف قضائي، كذلك يجوز للمحكمة الحكم بإغلاقه بشكل مؤقت أو دائم، ولها أيضًا الحكم بحله وتصفيته، وأخيرًا لها أن تحكم بنشر الحكم في جريدتين رسميتين على نفقة الشخص المعنوي)

الخاتمة

انتهى البحث إلى جملة من النتائج والتوصيات، ويمكن إجمالها في التالي:

النتائج:

أولاً: خرج المشرع القطري عن الأحكام العامة المتعلقة بالمشاركة الإجرامية في جرائم غسل الأموال.

ثانيًا: خرج المشرع القطري عن الأحكام العامة المتعلقة بالشروع في جرائم غسل الأموال.

ثالثًا: خرج المشرع القطري عن الأحكام العامة المتعلقة بالارتباط بين الجرائم في جرائم غسل الأموال.

رابعًا: خرج المشرع القطري عن الأحكام العامة المتعلقة بسريان القانون من حيث المكان في جرائم غسل الأموال.

خامسًا: خرج المشرع القطري عن الأحكام العامة بشأن عقوبة الشخص المعنوي في جرائم غسل الأموال.

التوصيات:

أولاً: نقترح على المشرع القطري بإعادة النظر في أحكام المادة 17 من قانون العقوبات القطري، وذلك بشمول جرائم غسل الأموال وتمويل الإرهاب بمبدأ عالمية النص الجنائي، توفيقًا مع أحكام المادة 94 من قانون غسل الأموال وتمويل الإرهاب رقم 20 لسنة 2019.

ثانيًا: نقترح إعادة النظر أحكام المادة 37 من قانون العقوبات القطري بشأن عقوبة الشخص المعنوي لإزالة التعارض الدستوري الذي تضمنته المادة 37 المتمثل بمنح القاضي الجنائي صلاحية اختيار "ما يتناسب من عقوبات" بشأن الشخص المعنوي.

ثالثًا: ضرورة التدخل التشريعي لاستبعاد التقادم الجنائي من التطبيق على جرائم غسل الأموال، أو على الأقل إطالة مدة التقادم فيها؛ وذلك للمواءمة بين أحكام اتفاقية الأمم المتحدة لمكافحة الفساد لسنة 2003 والتي صادقت عليها دولة قطر وبين أحكام قانون مكافحة جرائم غسل الأموال.

رابعًا: نقترح إعادة صياغة نص الفقرة 4 من المادة 2 من قانون مكافحة جرائم غسل الأموال، فالمساعدة أو التحريض أو التسهيل أو تقديم المشورة أو التعاون أو المساهمة كلها ذات معنى الاشتراك، وعليه نقترح على المشرع القطري ترشيد الفقرة آنفة الذكر وإزالة ما ورد فيها من تكرار أو زيادة.

قائمة المراجع

المراجع العربية:

- الضمور، باسل عبد الله، غسل الأموال في المصارف، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض 2013.
- الوكيل، محمد، مكافحة جريمة غسل الأموال في المملكة العربية السعودية، مكتبة القانون والاقتصاد، الرياض (2015).
- إسماعيل، سمر فايز، تبييض الأموال، منشورات زين الحقوقية، لبنان، 2010.
- الأشقر، منى، تبيض الأموال الناتجة عن الاتجار غير المشروع بالمخدرات/ مركز المعلوماتية القانونية – الجامعة اللبنانية (1995).
- العمري، عزت محمد، جريمة غسل الأموال، ط1، دار النهضة العربية، مصر، (2006).
- العريان، محمد علي، عمليات غسيل الأموال وآليات مكافحتها، دار الجامعة الجديدة للنشر، الإسكندرية، (2005).
- الدليمي، مفيد نايف، غسيل الأموال في القانون الجنائي، دار الثقافة للنشر والتوزيع، ط1، عمان، الأردن، (2005).
- جاسم، عمار باسل، جريمة غسل الأموال في القانون العراقي، عالم المعرفة للكتاب، بغداد، 2011.
- نبيلة، قيشان، الدور الوقائي للبنك في مكافحة تبيض الأموال، دار الأيام للطباعة والنشر، عمان، (2017).
- عبود، سالم محمد، ظاهرة غسيل الأموال –المشكلة والآثار، دار الدكتور للعلوم الإدارية والاقتصادية، بغداد، الطبعة (2013)
- غنام، غنام محمد، شرح قانون العقوبات القطري الأحكام العامة، الطبعة الأولى، منشورات كلية القانون، جامعة قطر (2017).
- شمس الدين، أشرف، شرح قانون العقوبات القطري –القسم العام، منشورات جامعة قطر– كلية القانون، الطبعة الأولى (2010).
- النقرش، أمجد، البنيان القانوني لجريمة غسل الأموال، المجلة القانونية، العدد الخامس، البحرين، (2016).
- الحاجي، عمر، غسيل الأموال، دار المكتبي، الطبعة الأولى، دمشق (2005).

المراجع الإنجليزية:

- History of Anti-Money Laundering Laws". United States Department of the Treasury. 30 June 2015. Archived from the original on 8 December 2016. Retrieved 30 June 2015. Money laundering - Wikipedia
- LexisNexis website, https://www.lexisnexis.co.uk/legal/guidance/what-types-of-offences-under-the-proceeds-of-crime-act-2002-poca-2002-should-lawyers-who-are-acting-in
- France Penal Code Article 324- (Act no. 96-392 of 13th May 1996 Article 1 Official Journal of 14th May 1996), (Ordinance no. 2000-916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January 2002)
- Crime of money laundering in Qatari Law: Definition and Elements: A Comparative Study" Sami Hamdan
- Al-Rawashdah (2020) Vol. 23, Issue 5, Journal of Legal, Ethical and Regulatory Issues (Scopus, Q2)
- Criminal Liability for the Crime of Money Laundering and the Regulator Framework for Combating It in Qatari Law" Sami Hamdan Al-rawashdah (2022) Vol. 25, Special Issue 1, Journal of Legal, Ethical and Regulatory Issues Scopus, Q2

حجيّة الأحكام الجنائيّة أمام سلطات التأديب

دراسة تحليليّة مقارنة بين القانون القطريّ والقانون المصريّ

مريم عبدالله العون

ماجستير في القانون العام - جامعة قطر / باحث قانوني في مجلس التأديب الابتدائي - وزارة الداخلية، قطر

حجيّة الأحكام الجنائيّة أمام سلطات التأديب
دراسة تحليليّة مقارنة بين القانون القطريّ والقانون المصريّ

مريم عبد الله العون
ماجستير في القانون العام- جامعة قطر / باحث قانوني في مجلس التأديب الابتدائي - وزارة الداخلية، قطر

المُلخَّص

يناقش هذا البحث حجيّة الحكم الجنائيّ أمام سلطات التأديب عند مساءلة الموظّف تأديبيًا في القانون القطريّ والقانون المصريّ، وذلك من خلال إجراء مقارنة بين هذين القانونيّين، وقد وقع الاختيار على القانون المصريّ بسبب كثرة الاجتهادات الفقهيّة والقضائيّة في مصر والتي تسعى إلى الوصول إلى أثر الأحكام الجنائيّة الصادرة بالإدانة أو بالبراءة على المساءلة التأديبيّة للموظّف العام، كما أنّ الأسانيد القانونيّة التي استندت إليها المحكمة الإداريّة في مصر للحكم بهذه المسائل تتشابه إلى حد كبير مع الأسانيد القانونيّة في القانون القطريّ بهذا الشأن، وبناءً عليه يقسم هذا البحث إلى مطلبين. تم تخصيص المطلب الأول للحديث عن مفهوم حجيّة الحكم الجنائيّ بشكل عام وأهم الشروط الواجب توفرها في الحكم ليكتسب الحجيّة، في حين يتناول المطلب الثاني نطاق حجيّة الحكم الجنائيّ أمام سلطات التأديب عند مساءلة الموظّف العام، من خلال فرعين: يناقش الفرع الأول حجيّة الحكم الجنائيّ الصادر بالبراءة أمام سلطات التأديب، وينتهي هذا الفرع إلى أنّ الحكم الجنائيّ الصادر بالبراءة لا يمنع في جميع الأحوال مساءلة الموظّف تأديبيًا، أما الفرع الثاني فتمّ تخصيصه للحديث عن حجيّة الحكم الجنائيّ الصادر بالإدانة أمام سلطات التأديب، والذي يبيّن أن له حجيّة مطلقة لا يجوز لسلطة التأديب بأي حال من الأحوال أن تحكم بخلاف ما جاء فيه أو تعاود البحث في صحة الواقعة التي أثبتها الحكم الجنائيّ.

الكلمات المفتاحية: موظّف عام، مساءلة تأديبيّة، تأديب، أثر، براءة، إدانة.

ABSTRACT

Authority of Criminal Judgments before Disciplinary Authorities – An Analytical Comparative Study between Qatari Law and Egyptian Law

Maryam Abdullah Alown

Master's degree in Public Law - Qatar University

Legal Researcher in Disciplinary Council - Ministry of Interior, Qatar

This research discusses the impact of criminal judgments on disciplinary authorities when an employee is subject to disciplinary proceedings under Qatari and Egyptian law, through a comparative analysis of these two legal systems. The choice of Egyptian law is based on the extensive doctrinal and judicial interpretations in Egypt, which seek to determine the effect of criminal judgments, whether of conviction or acquittal, on the disciplinary accountability of public employees. Additionally, the legal grounds relied upon by the Administrative Court in Egypt to rule on these matters are quite similar to the legal grounds in Qatari law on this subject. Based on this, the research is divided into two sections. The first section explains the concept of the legal authority for the criminal judgement generally as well as essential conditions that must be met for the judgement to be authoritative. The second section discusses the effect of the criminal judgement by the disciplinary authorities in the disciplinary trial of the public servant. This is done under two subsections: the first subsection discusses the authority for the criminal judgement of acquittal by the disciplinary authorities, finding that the criminal judgement of acquittal does not, in any circumstances, preclude the disciplinary trial of the public servant. The second subsection is about the legal authority for the criminal judgement of conviction by the disciplinary authorities whereby it is clearly established that such judgement has an absolute authority, which the disciplinary authority is not allowed, in any circumstances, to make a contrary judgement or seek to investigate the incident, which the criminal judgement has earlier confirmed.

Keywords: Public employee, Disciplinary Trial, Discipline, Effect, Acquittal, Conviction.

المقدمة:

تُعد الوظيفة العامة خدمة وطنيّة شريفة، يلتزم متولّيها بمراعاة المصلحة العامة وحدها، والالتزام التام بكافّة الواجبات التي تمليها عليه وظيفته، باعتبار أن الوظيفة العامة تكليفًا وليس تشريفًا، وقد أكّد الدستور القطريّ أهميّة الوظيفة العامة في مادته الرابعة والخمسين والتي تنصّ على «الوظائف العامة خدمة وطنيّة، ويستهدف الموظّف العام في أداء واجبات وظيفته المصلحة العامة وحدها».

ومثلما تقرر القوانين المنظمة للوظيفة العامة حقوق وواجبات الموظّف، فإنّها تقرر كذلك الجزاءات التأديبيّة المترتبة على مخالفة هذه الواجبات، وعليه فإذا أخلّ الموظّف بأحد هذه الواجبات وجد نفسه بمواجهة المساءلة التأديبيّة، وفي العديد من الأحوال يشكّل فعل الموظّف جريمة جنائيّة، ومخالفة تأديبيّة، فيصبح الأخير بمواجهة مسؤوليتين عن فعله الآثم، مسؤوليّة جنائيّة ومسؤوليّة تأديبيّة، وعلى الرغم من استقلال المسؤوليّة التأديبيّة عن المسؤوليّة الجنائيّة، إلا أنّ هناك حالات تلتزم بها جهات التأديب بعدم مخالفة ما توصّل إليه الحكم القضائيّ من براءة أو إدانة.

ولا يفوتنا أن نشير إلى أن موضوع تأديب الموظّف العام محل اهتمام للعديد من الباحثين في مجال القانون الإداريّ، وتناولته العديد من الدراسات والبحوث من كافة الزوايا، ومن ثمّ من الصعب الإلمام بجوانبه كافة؛ لذا ركّز هذا البحث على حجيّة الحكم الجنائيّ أمام سلطات التأديب، وفي سياق الحديث عن حجيّة الحكم الجنائيّ، لا بد من التطرّق مسبقًا إلى مفهوم حجيّة الحكم الجنائيّ، وشروط اكتساب الحكم للحجيّة.

أهميّة البحث:

تكمن أهميّة البحث في حجيّة الحكم الجنائيّ أمام سلطات التأديب في أن كلتا المسؤوليتين الجنائيّة والتأديبيّة تقومان على السبب نفسه؛ ما يدل على أن هناك ارتباطًا وثيقًا بينهما، وباعتبار أنّ المحاكم الجنائيّة هي صاحبة الاختصاص الأصيل في محاكمة المتهم، والبحث في مدى صحة الاتهام المنسوب إليه، فإنّه من المؤكد أن ما توصّلت إليه من نتائج لا يجوز نقضه من قِبل سلطات أخرى تحقّق في صحة الفعل ذاته، وعليه كان من اللازم البحث في مدى حجيّة الحكم الجنائيّ أمام سلطات التأديب ومدى وجوب التزامها بما توصّل إليه من نتائج، لضمان احترام وحجيّة الأحكام الجنائيّة.

كما تكمن أهميّة هذا البحث في كونه يجري مقارنة بين قانونين متشابهين في التنظيم القانونيّ لحجيّة الأحكام الجنائيّة، وهما القانون القطريّ والقانون المصريّ، إلا أنّ هذا الأخير متقدّم على الأول بكثرة الاجتهادات الفقهيّة والقضائيّة التي تسعى إلى تفسير النصوص القانونيّة للوصول إلى إجابات واضحة حول حجيّة الحكم الجنائيّ على المساءلة التأديبيّة للموظّف العام، وهو الأمر الذي يقودنا إلى تحقيق هدف البحث والمتمثّل في معرفة مدى كفاية التنظيم القانونيّ لحجيّة الحكم الجنائيّ على المساءلة التأديبيّة في القانون القطريّ في ضوء القانون المصريّ.

إشكالية وتساؤلات البحث:

تكمن الإشكالية الأولى في أن المسؤوليّة التأديبيّة مستقلة استقلالاً تامًا عن المسؤوليّة الجنائيّة، باعتبار أنّ الأولى قائمة على تهمة مستقلّة عن التهمة الجنائيّة، حتى وإن كانت هاتان المسؤوليتان قائمتين على السبب نفسه، وأنّ للحكم الجنائيّ حجيّة مطلقة بمواجهة الكافّة، فلا يجوز لأيّ جهة إثبات عكس ما جاء به وما توصل إليه من نتائج، ومن هذا المنطلق تظهر الإشكاليّة الأولى والتي تتمثّل في مفهوم حجيّة الحكم الجنائيّ والشروط الواجب توفرها في الحكم الجنائيّ ليكتسب الحجيّة أمام سلطة التأديب، خاصّة أنّ سلطة التأديب سلطة مستقلّة كما ذكرنا مسبقًا، وبناء عليه، تثير هذه الإشكاليّة الأسئلة التالية التي ستتمّ الإجابة عليها من منظور القانون القطريّ والقانون المصريّ من خلال استعراض وتحليل النصوص القانونيّة المتعلقة بهذا الشأن

- ما مفهوم حجيّة الأحكام الجنائيّة؟
- ما شروط اكتساب الحكم الجنائيّ للحجيّة؟

أما الإشكاليّة الثانية فتتعلق بنوع الأحكام القضائيّة ذات الحجيّة، لا سيما وأنّ الأحكام القضائيّة ليست على شاكلة واحدة، فمنها ما يصدر بالإدانة، ومنها ما يصدر بالبراءة، وباعتبار أنّ المشرع القطريّ لم ينظّم أثر حجيّة الحكم الجنائيّ على المساءلة التأديبيّة بنص خاص، فإن هذا الأمر دفعنا للبحث في النصوص القانونيّة العامة، والاجتهادات القضائيّة القطريّة، ومقارنتها بالنصوص القانونيّة، والاجتهادات القضائيّة والفقهيّة المصريّة؛ وذلك للتمكن من معرفة مدى كفاية التنظيم القانونيّ والاجتهاد القضائيّ لحجيّة الحكم الجنائيّ أمام سلطات التأديب في القانون القطريّ، وبناء على ذلك تفرعت من هذه الإشكالية الأسئلة التالية:

- ما مدى حجيّة الحكم الجنائيّ الصادر بالبراءة أمام سلطات التأديب؟
- ما مدى حجيّة الحكم الجنائيّ الصادر بالإدانة أمام سلطات التأديب؟

الدراسات السابقة:

- عوامله، عمر سلمان محمد، حجيّة الحكم الجنائيّ أمام سلطات التأديب- دراسة مقارنة بين مصر والأردن، رسالة دكتوراه (جامعة العلوم الإسلاميّة العالميّة)، الأردن، 2014.

تناولت هذه الدراسة حجيّة الحكم الجنائيّ أمام سلطات التأديب في القانون الأردنيّ مقارنة بالقانون المصريّ، وقد أثار الباحث عدة أسئلة تتعلق بمدى وجوب معاقبة الموظّف تأديبيًا بعد معاقبته جنائيًا على الفعل ذاته، بالإضافة إلى تقييد الحكم الجنائيّ لسلطة التأديب بما حكم به من براءة أو إدانة، وناقشت الدراسة كذلك مدى حقّ سلطة التأديب بالالتفات عن الحكم القضائيّ في بعض المسائل، وخلصت الدراسة إلى عدة توصيات للمشرّع الأردنيّ، ومن أهمها: ضرورة وجود نصّ تشريعيّ ينظم حجيّة الحكم الجنائيّ أمام سلطات التأديب.

- العجاج، مصون طلال، أثر الحكم الجزائيّ على تأديب الموظّف العام، رسالة ماجستير، كلية القانون (جامعة اليرموك)، الأردن، 2015م.

ناقشت هذه الدراسة أثر الأحكام القضائيّة الصادرة بالبراءة أو الإدانة أو عدم المسؤوليّة على تأديب الموظّف العام، وبينت مدول المخالفة التأديبيّة والجريمة الجنائيّة، وأوجه التشابه والاستقلال بينهما، وذلك من خلال الرجوع إلى الأنظمة والقوانين التي عالجت تلك المواضيع، بالإضافة إلى الآراء الفقهيّة والاجتهادات القضائيّة بهذا الشأن، وتوصلت الدراسة إلى عدّة توصيات للمشرع الأردنيّ، من أهمها: إعادة النظر في نصوص نظام الخدمة المدنيّة الحالي وتعديلها بما يتسق مع قانون العقوبات، خاصّة في عقوبة العزل، كما أوصت الدراسة بضرورة النصّ في نظام الخدمة المدنيّة على وجوب احترام حجيّة الحكم الجنائيّ من قِبل سلطات التأديب منعًا لتضارب الأحكام.

- هنداوي، السيد فتوح محمد، أثر الحكم الجنائيّ على المسؤوليّة التأديبيّة للموظّف العام في النظام القانونيّ السعوديّ، مجلة البحوث الاقتصاديّة والقانونيّة، ع24، مصر، 2020.

سلّطت هذه الدراسة الضوء على ما تضمنته أحكام هيئة التأديب وديوان المظالم السعوديّ من مبادئ وأسس تتعلق بتحديد نطاق العلاقة بين المسؤوليّة التأديبيّة والمسؤوليّة الجنائيّة؛ وذلك لمقارنتها مع الأحكام القضائيّة الصادرة من القضاء الإداريّ المصريّ؛ وذلك لتحديد نطاق أثر الحكم الجنائيّ الصادر في المسؤوليّة الجنائيّة على المسؤوليّة التأديبيّة، وتوصّلت الدراسة إلى عدة توصيات لكل من المشرع السعوديّ، والجهات التأديبيّة، تتمثل أولاً في توصية المشرع بضرورة تعديل بعض أحكام لائحة انتهاء خدمة الموظّف وثانيًا بتوصية جهة التأديب بضرورة الاستئناس بالأحكام القضائيّة عند الحكم بعقوبة تأديبيّة على الموظّف العام.

- الكبيسي، مها خليفة راشد، أثر الحكم الجنائيّ على المسؤوليّة التأديبيّة للوظف العام في التشريع القطريّ: دراسة مقارنة، رسالة ماجستير، كلية القانون (جامعة قطر)، قطر، 2021.

تناولت هذه الدراسة أثر الحكم الجنائيّ الصادر ضد الموظّف العام على مسؤوليته التأديبيّة، وعالجت هذه الدراسة إشكالية تحديد الإطار القانونيّ الذي ينظم علاقة الجريمة الجنائيّة بالجريمة التأديبيّة، من خلال بيان حجيّة الأحكام الجنائيّة الصادرة ضد الموظّف العام أمام سلطات التأديب، وذلك في ضوء القانون القطريّ مقارنة بالقانون المصريّ، وقد توصلت الدراسة إلى عدة نتائج وتوصيات، من أهمّها ضرورة تصدّي المشرّع القطريّ لحجيّة الأحكام الجنائيّة أمام سلطات التأديب من خلال تقنينها.

منهج البحث:

انتهج هذا البحث المنهج التحليليّ والمنهج المقارن؛ إذ تمّ تحليل النصوص القانونيّة المتعلّقة بحجيّة الحكم الجنائيّ في القانون القطريّ، ومن ثمّ استعراض الاجتهادات القضائيّة والفقهيّة المتعلقة بحجيّة الحكم الجنائيّ على المساءلة التأديبيّة للوقوف على مدى فعاليتها في غياب النصّ القانونيّ بهذا الشأن، ومن ثمّ تمّت مقارنتها بالنصوص القانونيّة والاجتهادات الفقهيّة والقضائيّة في القانون المصريّ؛ نظرًا لوضوح الاجتهاد القضائيّ والفقهيّ في مصر بهذا الشأن، ومن ثمّ فإنّ هذا الأمر سوف يسهم في تطوير التنظيم القانونيّ لحجيّة الحكم الجنائيّ على المساءلة التأديبيّة في القانون القطريّ.

خطة البحث:

تمّ تقسيم البحث إلى مطلبين يحتوي كل مطلب على فرعين، وفق ما يلي:

- **المقدمة.**
- **المطلب الأول: ماهية الأحكام الجنائيّة ذات الحجيّة:**
  - الفرع الأول: مفهوم حجيّة الأحكام الجنائيّة.
  - الفرع الثاني: شروط اكتساب الحكم للحجيّة.
- **المطلب الثاني: نطاق حجيّة الحكم الجنائيّ أمام سلطات التأديب:**
  - الفرع الأول: حجيّة الحكم الجنائيّ الصادر بالبراءة على سلطات التأديب.
  - الفرع الثاني: حجيّة الحكم الجنائيّ الصادر بالإدانة على سلطات التأديب.
- **خاتمة (نتائج وتوصيات).**

المطلب الأول

ماهية الأحكام الجنائيّة ذات الحجيّة

يُعدّ الحكم الجنائيّ خلاصة عمل واجتهاد القاضي، فمن خلال البحث في صحة الوقائع وتكييفها ونسبتها إلى المتهم يصدر القاضي حكمه فيما توصلّت إليه قناعته، وهذا الحكم يُعد فاصلاً في المنازعة ويلزم الخصوم وكافة الجهات القضائيّة وغير القضائيّة بترك البحث فيما قضى به والتسليم لما جاء به واحترامه،[1] فلا يجوز للجهات الأخرى أن تعاود البحث في صحة مسألة فصل فيها الحكم الجنائيّ، بل وتلتزم كل جهة تنظر في دعوى مرتبطة بالدعوى الجنائيّة ألا تحكم بما يخالف ما جاء في الحكم الجنائيّ سواء كان الحكم الصادر بالإدانة أم بالبراءة. ومن هنا تظهر فكرة حجيّة الحكم القضائيّ الجنائيّ، والتي تبناها الفقه والقضاء وكذلك التشريعات، وأثرها في السلطات التي تنظر في موضوع مرتبط بموضوع الدعوى الجنائيّة، وقد تناول هذا المطلب مفهوم حجيّة الحكم الجنائيّ وبيان الآثار المترتّبة على الحجيّة في الفرع الأول، ومن ثمّ ناقش الشروط الواجب توفرها لتمتّع الحكم بهذه الحجيّة في الفرع الثاني.

الفرع الأول: مفهوم حجيّة الحكم الجنائيّ وآثارها

الحجيّة لغة: هي البرهان، وقيل: ما دوفع به الخصم؛ وقال الأزهري: الحجّة الوجه الذي يكون به الظفر عند الخصومة.[2]

الحجيّة اصطلاحًا: حجيّة الحكم تعني أنّ للحكم حجيّة فيما بين الخصوم، وبالنسبة إلى ذات الحق محلاً وسببًا. فيكون الحكم حجّة في هذه الحدود، حجّة لا تقبل الدحض ولا تتزحزح إلا بطريق من طرق الطعن في الحكم. وتثبت هذه الحجيّة لكل حكم قطعي، أي لكل حكم موضوعي يفصل في خصومة، وتبقى للحكم حجيته إلى أن يزول، فإن كان غيابيًا يزول بإلغائه في المعارضة، وإن كان ابتدائيًا يزول بإلغائه في الاستئناف، وإن كان نهائيًا يزول بنقضه أو بقبول التماس إعادة النظر فيه.

وتجد حجيّة الحكم الجنائيّ سندها في نصوص القوانين كذلك، فبالنسبة للمشرع القطريّ فقد نصّت المادة (319) من قانون الإجراءات الجنائيّة القطريّ على أنه: (يكون للحكم الجنائيّ البات الصادر في موضوع الدعوى الجنائيّة بالإدانة حجيّة تلتزم بها المحاكم

(1) عنيبة، علي محمد علي، حجيّة الحكم الجنائي أمام القضاء المدني، مجلة البحوث القانونيّة، المجلد الثالث، العدد الثاني، جامعة مصراتة، ليبيا، 2016م، ص167.

(2) ابن منظور، لسان العرب، المجلد الثالث (ح)، ج3،، الطبعة الثانية، دار إحياء التراث العربي، بيروت- لبنان، 1993، ص53.

المدنية في الدعاوى التي لم تكن قد فصلت فيها بحكم بات، فيما يتعلق بوقوع الجريمة وبوصفها القانونيّ ونسبتها إلى فاعلها. ويكون للحكم بالبراءة هذه القوة سواءً بني على انتفاء التهمة أم عدم كفاية الأدلة، ولا تكون له هذه القوة إذا كان مبنيًا على واقعة لا يعاقب عليها القانون).

ويلاحظ أن النص في القانون القطريّ مطابق لنص القانون المصريّ في المادة (456)؛ إذ نصت على أن (يكون للحكم الجنائيّ الصادر من المحكمة الجنائيّة في موضوع الدعوى الجنائيّة بالبراءة أو الإدانة قوة الشيء المحكوم به أمام المحاكم المدنية في الدعاوى التي لم يكن قد فصل فيها نهائيًا فيما يتعلق بوقوع الجريمة وبوصفها القانونيّ ونسبتها إلى فاعلها. ويكون للحكم بالبراءة هذه القوة سواء بني على انتفاء التهمة أم على عدم كفاية الأدلة. ولا تكون له هذه القوة إذا كان مبنيًا على أن الفعل لا يعاقب عليه القانون).[3]

ويستشف مما سبق أن كلاً من القانون القطريّ والقانون المصريّ قد اتفقا على أن الحكم الصادر في الدعوى عنوان للحقيقة، ولا يجوز للمحكمة التي أصدرته أو أي جهة أخرى قضائيّة أو غير قضائيّة أن تعيد النظر فيما فصل فيه الحكم الجنائيّ، أو إصدار حكم يتعارض معه.

ويتضح كذلك بأن اكتساب الحكم الجنائيّ للحجيّة في كلا القانونين يترتب عليه أثران أحدهما سلبي والآخر إيجابي. أما السلبي فيمنع كل محكمة أو جهة قضائيّة أخرى من إعادة النظر في الواقعة التي فصل فيها الحكم الجنائيّ، إذا تعلقت بالواقعة والخصوم ذاتهم، وذلك وفقًا لمبدأ عدم جواز معاقبة الشخص على فعل واحد مرتين والذي رددته الأنظمة القانونيّة المختلفة. ويسري هذا المبدأ حتى وإن كانت المحاكمة التالية للحكم الذي حاز الحجيّة قد تمت تحت وصف قانونيّ مختلف.[4]

وتطبيقًا لذلك قضت محكمة التمييز القطريّة في حكم لها «لما كان طرح واقعة إقامة الطاعن مظلة خارجية في غير الأحوال المرخص بها قانونًا بوصف أنها بناء بدون ترخيص وصدور حكم نهائي ببراءته منها تأسيسًا على عدم ثبوت التهمة -على سياق ما تقدم- يمنع من إعادة محاكمته عن الواقعة ذاتها بوصف جديد لما هو مقرر من أنه لا يجوز الرجوع إلى الدعوى الجنائيّة بعد الحكم فيها نهائيًا بناء على تغيير الوصف القانونيّ للجريمة وذلك طبقًا للمادة

(3) قانون الإجراءات الجنائيّة المصريّ رقم 150 لسنة 1950 والمعدل في سبتمبر 2020.

(4) هنداوي، السيد فتوح محمد، أثر الحكم الجنائي على المسؤوليّة التأديبيّة للموظّف العام في النظام القانونيّ السعودي، مجلة البحوث الاقتصادية والقانونيّة، ع24، جامعة المنصورة، مصر، 2020، ص238.

(318) من قانون الإجراءات الجنائيّة فإنه لا يجوز طرح الدعوى من جديد عن ذات الفعل وضد ذات الطاعن المحكوم ببراءته. لما كان ما تقدم، فإن المحكمة إذا رفضت الدفع بعدم جواز نظر الدعوى وعادت إلى نظر الدعوى بوصف آخر للفعل وفصلت في موضوعها من جديد بالنسبة للطاعن بعد أن زالت ولايتها بإصدار الحكم الأول ببراءته يكون حكمها المطعون فيه قد أخطأ في القانون خطأ يؤذن لهذه المحكمة- عملاً بالمادة (292) من قانون الإجراءات الجنائيّة- أن تصحح الحكم على مقتضى القانون بالقضاء بإلغاء الحكم المستأنف والقضاء بعدم جواز النظر في الدعوى لسبق الفصل فيها نهائيًا».[5]

كما أكد القضاء المصريّ ذلك في أحد أحكامه والذي جاء فيه أن «على ما جرى به قضاء محكمة النقض أنه يحظر محاكمة الشخص عن الفعل ذاته مرتين، وأنه إذا رفعت الدعوى عن واقعة معينة بوصف معين وحكم فيها فلا يجوز بعد ذلك رفع الدعوى عن تلك الواقعة ذاتها بوصف جديد ومناط الواقعة التي تمنع من إعادة المحاكمة -ولو تحت وصف جديد- أن يتحد الأساس الذي أقيمت عليه الوقائع في الدعويين، بمعنى ألا يكون لكل دعوى ذاتية مستقلة وظروف خاصة تتحقق بها الغيرية التي يمتنع معها القول بوحدة السبب فيهم».[6]

أما الأثر الإيجابي لحجيّة الحكم الجنائيّ فيتمثل في افتراض الحقيقة فيما قضى به الحكم وانتهاء الدعوى الجنائيّة بكل عناصرها الشخصية والموضوعية.[7]

وأفصحت المادة 317 من قانون الإجراءات الجنائيّة القطريّ عن هذا الأثر بقولها «تنقضي الدعوى الجنائيّة، بالنسبة للمتهم المرفوعة عليه والوقائع المسندة فيها إليه، بصدور حكم بات بالبراءة أو الإدانة». ونصت على ذلك المادة 454 من قانون الإجراءات الجنائيّة المصريّ.[8]

وبالمقابل هناك العديد من التشريعات التي لم تنص على ذلك صراحة ومنها المشرع اللبناني؛ إذ يرى أنه لا حاجة للنص عليه باعتبار أنه نتيجة بديهية ومنطقية لكون الحكم الجنائيّ قد حاز لحجيّة الأمر المقضي.[9]

(5) محكمة التمييز القطريّة، جنائي، الطعن رقم202 لسنة 2013، جلسة 18-11-2018.

(6) محكمة النقض المصريّة، جنائي، الطعن رقم 23634، لسنة 67ق، جلسة 2-6-1998

(7) بهساوي، خالد صفوت ناجي، الحجيّة السلبية للحكم الجنائي الأجنبي: دراسة تحليلية مقارنة في القانون المصريّ والفرنسي، مجلة العلوم القانونيّة والاقتصادية، مج62، ع1، جامعة عين شمس، مصر، 2020م

(8) قانون رقم 150 لسنة 1950 بشأن قانون الإجراءات الجنائيّة، المادة 454.

(9) د. ثروت، جلال، د. عبد المنعم، سليمان، أصول المحاكمات الجزائية – الدعوى الجنائيّة، الطبعة الأولى، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت- لبنان، 1996م، ص267

الفرع الثاني: شروط اكتساب الحكم الجنائيّ للحجيّة

حتى يكتسب الحكم الجنائيّ الحجيّة وينتج الآثار المترتبة عليه، لا سيما أمام سلطات التأديب لا بد أن تتوفر فيه عدة شروط، نجمعها بالتالي: أولها أن يصدر من جهة قضائيّة وطنية مختصة. ثانيها أن يصدر الحكم في مسألة جنائيّة ويكون فاصلاً في الدعوى. ثالثها: أن يكون الحكم الجنائيّ سابقًا على الفصل بالدعوى التأديبيّة، وآخرها: أن يكون الحكم باتًّا غير قابل للطعن فيه.

أولاً: صدور الحكم الجنائيّ من جهة قضائيّة وطنية:

حتى يتمتع الحكم الجنائيّ بحجيته أمام الجهات القضائيّة وسلطات التأديب تحديدًا، لا بد من صدوره من القضاء المختص ليكون هو القرار الحاسم الذي تنقضي به الدعوى، فأي قرار يصدر من جهة أخرى حتى وإن كان متعلقًا بالدعوى الجنائيّة لا يكتسب الحجيّة ولا يرتب آثارها، كقرار حفظ الأوراق الصادر من النيابة العامة، أو قرار عدم المحاكمة وغيره من القرارات الأخرى.[10]

وقد حدد الدستور القطريّ لسنة 2004 الأسس التي يقوم عليها النظام القضائيّ القطريّ، وترك أمر تنظيمها للقوانين الخاصة، وبناء عليه صدر قانون السلطة القضائيّة رقم (10) لسنة (2003)، وقرر توحيد الجهات المختصة بنظر المنازعات وأطلق عليها اسم المحاكم، وهي المحكمة الابتدائيّة، ومحكمة الاستئناف، ومحكمة التمييز، لتختص كل منها بالفصل في المسائل والمنازعات المرفوعة إليها طبقًا للقانون.

كما يقتضي صدور الحكم من محكمة وطنيّة وفقًا لمبدأ الإقليميّة في القانون الجنائيّ والذي يترتّب عليه عدم سريان قانون الدولة وأحكامها إلا في حدود إقليمها ولا تمتد الآثار الجنائيّة إلى إقليم دولة أخرى؛ لذا فإنّه ليس للأحكام الأجنبيّة أي حجيّة أو قوة تنفيذيّة في مواجهة السلطات الوطنيّة إلا إذا كان هناك اتفاق بين الدولتين بموجب معاهدة دوليّة يعطي أحكام الدولة الأجنبيّة الحجيّة والقوة التنفيذيّة في إقليم الدولة، ومع ذلك ليس هناك ما يمنع سلطة التأديب من الاستعانة بالحكم الأجنبيّ كدليل اتهام شأنه شأن الأدلة الأخرى[11].

(10) ثروت، جلال، د. عبد المنعم، سليمان، المرجع السابق، ص264.

(11) انظر: نويجي، محمد فوزي، حجيّة الأحكام الجنائيّة على الجريمة التأديبيّة في ضوء القانون القطريّ، المجلة القانونيّة والقضائيّة، ع1، قطر، 2021، ص124. غنام، طارق فيصل، العلاقة بين الجريمة التأديبيّة والجريمة الجنائيّة: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا (جامعة النجاح الوطنية)، فلسطين، 2016، ص97

ثانيًا: صدور الحكم في مسألة جنائيّة وأن يكون فاصلاً في موضوع الدعوى:

يشترط حتى يتمتع الحكم الجنائيّ بالحجيّة أن يصدر في مسألة جنائيّة، أي فعل يجرمه القانون ويقرر له عقوبة معينة، وسواء صدر الحكم بالإدانة أم بالبراءة، ويستوي أن يكون الحكم قد صدر من المحكمة الجنائيّة بصفتها صاحبة الاختصاص الأصيل، أو من المحكمة المدنية بصورة استثنائية[12]، كما تعد الأحكام الصادرة من الجهات الإداريّة ذات الاختصاص القضائيّ أحكامًا جنائيّة تحوز حجيّة الأمر المقضي طالما كان الحكم قد فصّل بمسألة جنائيّة.[13]

ويشترط كذلك أن يكون الحكم فاصلاً في موضوع الدعوى، بمعنى أن يكون منهيًا للدعوى الجنائيّة وفاصلاً في الخصومة سواء بإدانة المتهم وتوقيع العقوبة عليه أم ببراءته مما نسب إليه، وإذا كان سير الدعوى يقتضي صدور أحكام سابقة على الحكم الفاصل كالأحكام التمهيدية أو الأحكام الصادرة في الدفوع الفردية، وكذلك الأحكام المبدئية والمتعلقة بشكل الدعوى كبطلان الإعلان، أو عدم قبول الدعوى فإن هذه الأحكام كافة ليس لها حجيّة أمام سلطات التأديب؛ إذ لا تعد أحكامًا فاصلة في موضوع الدعوى ومنهية للخصومة، وكذلك قرارات النيابة العامة كالأمر بحفظ أوراق الدعوى أو الأمر بالأوجه لإقامة الدعوى، ووحده الحكم الفاصل يكتسب حجيّة الأمر المقضي.[14]

ثالثًا: أن يكون الحكم الجنائيّ سابقًا على الفصل في الدعوى التأديبيّة:

رغم استقلال الدعوى التأديبيّة عن الدعوى الجنائيّة استقلالاً تامًا، إلا أنّ هذا الاستقلال لا يمنع من تقيد السلطات التأديبيّة بما توصل إليه الحكم الجنائيّ من صحة أو نفي الوقائع ونسبتها إلى المتهم طالما أنّ الفعل يشكل جريمة جنائيّة وجريمة تأديبيّة في الوقت ذاته، ومع ذلك يشترط في الحكم الجنائيّ حتى تتقيد به سلطات التأديب أن يكون صادرًا قبل صدور القرار التأديبي، أو قبل أن يصبح هذا الأخير باتًّا.[15]

---

(12) ومن الأحكام الجنائيّة التي تصدر من المحاكم المدنية بصورة استثنائية هي ما نص عليه قانون المرافعات المدنية القطريّ رقم 13 لسنة 1990 في المادة (1/60)، والتي جاء فيها: ضبط الجلسة وإدارتها منوطان برئيسها. ويكون له في سبيل ذلك أن يخرج من قاعة الجلسة من يخل بنظامها، فإن لم يمتثل وتمادى، كان للمحكمة أن تحكم على الفور بحسبه أربعًا وعشرين ساعة أو بغرامة لا تزيد على خمسمائة ريال، ويكون حكمها غير قابل للطعن). والمادة 65 والتي تنص على: (للمحكمة أن تحاكم من تقع منه أثناء انعقادها جنحة تعدّ على هيئتها أو على أحد أعضائها أو أحد العاملين بالمحكمة، وتحكم عليه فورًا بالعقوبة. وللمحكمة أيضًا أن تحاكم من شهد زورًا بالجلسة. وتحكم عليه بالعقوبة المقررة لشهادة الزور. ويكون حكم المحكمة في هذه الأحوال نافذًا ولو حصل استئنافه)

(13) نويجي، محمد فوزي، المرجع السابق، ص126.

(14) هنداوي، السيد فتوح محمد، مرجع سابق، ص248.

(15) نويجي، محمد فوزي، المرجع سابق، 123.

ويثار التساؤل حول حجيّة الحكم الجنائيّ الصادر بعد انتهاء الدعوى التأديبيّة؟

يرى غالبية الفقه والقضاء بأنّ حجيّة الحكم الجنائيّ مشروطة بصدوره قبل الفصل في الدعوى التأديبيّة بصورة نهائيّة، أما في حال صدر الحكم الجنائيّ بعد انتهاء الدعوى التأديبيّة فلا يكون له حجيّة في مواجهة سلطات التأديب حتى وإن كان مخالفًا لما توصلت إليه.[16]

وقد عالج المشرع القطريّ هذه الإشكالية ووضع نصوصًا تحد من حدوثها في قانون الموارد البشريّة؛ إذ أوجب على الإدارة أن تتوقف عن الإجراءات التأديبيّة في حال إحالة الموظّف إلى المحاكمة الجنائيّة إلى حين صدور حكم نهائي من المحكمة المختصة، وذلك ضمانًا لعدم تعارض الأحكام التأديبيّة مع الأحكام الجنائيّة.[17]

ومن جانبنا نرى بإعادة النظر في موقف المشرع القطريّ بتقييد الإدارة ومنعها من النظر في الدعوى التأديبيّة إلى حين صدور الحكم الجنائيّ؛ إذ يعد ذلك تقليلاً من دور القضاء التأديبي وتأخيرًا في إنهاء الدعوى التأديبيّة وعدم استقرار وضع الموظّف القانونيّ دون مبرر، خاصّة وأنّ المشرع اشترط أن يتم وقف الدعوى التأديبيّة إلى حين صدور الحكم النهائي في الدعوى الجنائيّة؛ ما يتسبب في طول مدة عدم استقرار وضع الموظّف القانونيّ، إذ ليس هناك جدوى من الانتظار خاصة إذا كانت الأدلة المقدمة للإدارة كافية لإثبات صحة الواقعة ونسبتها إلى الموظّف.

ولاعتبارات تتعلق باستقلال النظام التأديبي ومصلحة الموظّف نرى بأن الإدارة لا تلتزم بانتظار الحكم الجنائيّ لإصدار الحكم التأديبي.

وقد سلك المشرع القطريّ هذا الاتجاه في قانون الخدمة العسكرية رقم (31) لسنة 2006؛ إذ جعل الأمر جوازيًا للسلطة المختصة باستكمال إجراءات الدعوى أو وقفها حسب ما تراه مناسب، فنصّت المادة (78) على أنه «إذا تبين من التحقيق وجود شبهة جريمة، فعلى جهة التحقيق رفع الموضوع مشفوعًا بتوصيتها إلى السلطة المختصة أو من تفوضه بإحالة أوراق التحقيق إلى النيابة للتصرف فيه، وللسلطة المختصة أو من تفوضه أن تقرر استمرار إجراءات التأديب ضد العسكريّ أو وقفها لحين الفصل في الدعوى الجنائيّة».

ومن جانبنا لا نرى أنّ استمرار الإدارة في الدعوى التأديبيّة وعدم انتظارها للحكم الجنائيّ سوف يتسبب بتناقض بين الأحكام التأديبيّة والأحكام الجنائيّة ويؤثر على حجيتها، فمن

(16) المجدلاوي، مخيمر يوسف، حجيّة القرارات والأحكام الجزائية في المجال التأديبي: دراسة مقارنة بين القانونيّن المصريّ والفلسطيني، رسالة ماجستير، كلية الحقوق (جامعة الأزهر)، غزة س 2013، ص105

(17) المادة 105 من قانون الموارد البشرية رقم (15) لسنة (2016).

ناحية فإنّ الإدارة لن تستمر في الدعوى التأديبيّة إلا إذا وجدت بأنّ لديها أدلة كافية ووافية لإثبات صحة الواقعة ونسبتها إلى المتهم. ومن ناحية أخرى، فإنّ حجيّة الحكم الجنائيّ مقرونة بشرط صدوره قبل القرار التأديبي؛ ما يعني أن صدور القرار التأديبيّ قبل صدور الحكم الجنائيّ، أمرًا لا يجعل لهذا الأخير حجيّة بأثر رجعي على ما صدر من قرارات قبل اكتسابه للحجيّة.

رابعًا: أن يكون الحكم باتًا غير قابل للطعن:

يشترط حتى يحوز الحكم الجنائيّ الحجيّة أمام سلطات التأديب أن يكون باتًّا غير قابل للطعن سواء بالطرق العادية أم الطرق الاستثنائيّة.

ويقصد بالأحكام الباتّة هي تلك الأحكام التي تكون غير قابلة للطعن بأي طريق من طرق الطعن المقررة قانونًا، عدا طلب إعادة النظر.[18] والأحكام الباتّة وحدها من تحوز الحجيّة المطلقة أمام سلطات التأديب باعتبار ما توصلت إليه عنوانًا للحقيقة، أما الأحكام الابتدائيّة والنهائيّة فحجيّتها مؤقّتة تزول بإلغائها أو نقضها.

المطلب الثاني
نطاق حجيّة الحكم الجنائيّ أمام سلطات التأديب

لم تتطرق معظم التشريعات لحجيّة الحكم الجنائيّ أمام سلطات التأديب، على الرغم من تناولها لحجيته أمام المحاكم المدنية بشكل مفصّل، ومن هذه التشريعات التشريع القطريّ؛ إذ تناول حجيّة الحكم الجنائيّ أمام المحاكم المدنية في المادة (319) من قانون الإجراءات الجنائيّة[19]، كما تطرّق القانون المصريّ لهذه الحجيّة في المادة (456) من قانون الإجراءات الجنائيّة.[20]

(18) المادة 317 من قانون الإجراءات الجنائيّة القطريّ رقم (23) لسنة (2004).

(19) نص المادة (319): يكون للحكم الجنائي البات الصادر في موضوع الدعوى الجنائيّة بالإدانة حجيّة تلتزم بها المحاكم المدنية في الدعاوى التي لم تكن قد فصلت فيها بحكم بات، فيما يتعلق بوقوع الجريمة وبوصفها القانونيّ ونسبتها إلى فاعلها، ويكون للحكم بالبراءة هذه القوة سواءً بنى على انتفاء التهمة أو على عدم كفاية الأدلة، ولا تكون له هذه القوة إذا كان مبنيًا على أن الواقعة لا يعاقب عليها القانون

(20) نص المادة (456): «يكون للحكم الجنائي الصادر من المحكمة الجنائيّة في موضوع الدعوى الجنائيّة بالبراءة أو بالإدانة قوة الشيء المحكوم به أمام المحاكم المدنية في الدعاوى التي لم يكن قد فصل فيها نهائيًا فيما يتعلق بوقوع الجريمة وبوصفها القانونيّ ونسبتها إلى فاعلها. ويكون للحكم بالبراءة هذه القوة سواء بني على انتفاء التهمة أم على عدم كفاية الأدلة. ولا تكون له هذه القوة إذا كان مبنيًا على أن الفعل لا يعاقب عليه القانون»

لذا أولى الفقه والقضاء العناية البالغة والواسعة لهذا الأمر، وتوصلت الاجتهادات إلى أن للحكم الجنائيّ حجيّة أمام سلطات التأديب؛ إذ إنّ الدعوى التأديبيّة أقرب للدعوى الجنائيّة من الدعوى المدنيّة؛ إذ يتفقان بأنّ كليهما نظم عقابيّة تجرّم أو تخالف فعل وتقرر عقوبة على مرتكبه؛ لذا فإنّ كان للحكم الجنائيّ حجيّة في الدعوى المدنيّة، فمن باب أولى أن تكون له هذه الحجيّة في الدعوى التأديبيّة كذلك للسبب السابق ذكره.[21]

وقد أكّدت الاجتهادات القضائيّة ذلك؛ إذ جاء في حكم لمحكمة التمييز القطريّة أن «متى صدر الحكم صارت له حجيّة ملزمة وأصبح عنوانًا للحقيقة وصار نهائيًا غير قابل للطعن فيه، حاز قضاؤه قوة الأمر المقضي فيما فصل فيه بصفة صريحة أو ضمنية سواء في المنطوق أم في الأسباب المتصلة به اتصالاً وثيقًا لا يقوم بدونها، ولا يجوز لقضاء محكمة أن يتسلط على قضاء محكمة أخرى إلا إذا كانت أعلى درجة منها ومن خلال الطعن القضاء الأول في الأحوال وبالأوضاع المقررة قانونًا».[22]

وجدير بالذكر أن الحكم الجنائيّ لا يكتسب الحجيّة المطلقة بكل الأحوال؛ إذ فرقت التشريعات وكذلك الفقه والقضاء بين حجيّة الحكم الصادر بالإدانة وحجيّة الحكم الصادر بالبراءة.

وعليه انشغل هذا المطلب بتوضيح حجيّة كل منهما على المساءلة التأديبيّة للموظّف العام وذلك من خلال تقسيمه إلى فرعين، انشغل الفرع الأول ببيان حجيّة الحكم الجنائيّ الصادر بالبراءة على سلطات التأديب، في حين تناول الفرع الثاني حجيّة الحكم الجنائيّ الصادر بالإدانة على سلطة التأديب.

الفرع الأول: حجيّة الحكم الجنائيّ الصادر بالبراءة على سلطات التأديب

إن قرينة البراءة تعد من أهم المبادئ الدستوريّة والمبادئ العامة في القانون الجنائيّ، وأكد أهميتها الدستور القطريّ في نص المادة (39) والتي جاء فيها أن المتهم بريء حتى تثبت إدانته أمام القضاء، وتقوم هذه القرينة على اعتبار المتهم بريئًا حتى يصدر الحكم القضائيّ بإدانته، باعتبار البراءة هي الأصل في الإنسان.

إذن فالقاضي الجنائيّ حتى يحكم بالإدانة لا بد أن يصدر حكمه بناء على يقين وجزم تام يكفي معه نقض قرينة البراءة، وذلك بعكس الحكم بالبراءة والذي يتأسس بمجرد الشك في أدلة الإثبات، ولكون حكم البراءة يبنى على أسباب عدة، أولها: عدم كفاية الأدلة. وثانيها: عدم وجود الواقعة المادية. وثالثها: بطلان الإجراءات. ورابعها: انعدام المسؤوليّة الجنائيّة.

(21) غنام، طارق فيصل مصطفى، مرجع سابق، ص104.

(22) محكمة التمييز القطريّة، الطعن رقم 49 لسنة 1986 ق- جلسة 1986/3/20.

وخامسها: تخلف أحد أركان الجريمة الجنائيّة. وآخرها: شيوع التهمة. فإنّ الأمر يثير الجدل حول حجيّة الحكم الصادر بالبراءة أمام سلطات التأديب بتعدد حالاته، فيرى الفقه أنّ من الحالات ما تقيد سلطة التأديب وتمنعها من مساءلة المتهم، بينما لا تقيدها الحالات الأخرى وتترك لها سلطة التقدير، وسوف نبين حجيّة كل حالة على سلطة الإدارة على حدة.

أولاً: صدور حكم البراءة لعدم كفاية الأدلة:

عند عرض أدلة الإثبات أمام القاضي الجنائيّ يقوم بتمحيصها لتكوين عقيدته، فلا يحكم بالإدانة إلا بعد أن تتكون قناعته بالجزم واليقين بثبوت التهمة على المتهم، وما إن يزاوله مجرد شك في صحة الأدلة المقدمة ونسبتها إلى المتهم فيلتزم بطرحها جانبًا والحكم ببراءة المتهم وفقًا لمبدأ قرينة البراءة.[23]

وإن كان للحكم الصادر بالبراءة لعدم كفاية الأدلة حجيّة مطلقة أمام المحاكم المدنية في القانون القطريّ وكذلك القانون المصريّ، فاتجه غالبية الفقه والقضاء إلى أن ليس لهذا الحكم حجيّة أمام سلطات التأديب، وطالما أن الحكم بالبراءة صدر بسبب يعود لقناعة القاضي الوجدانية، فإن لسلطة التأديب كذلك الحق في تمحيص وتقدير الأدلة وتكوين عقيدتها على ما تم طرحه أمامها من أدلة لتقدر مدى ثبوت ارتكاب المتهم للمخالفة التأديبيّة، وفي حال رأت سلطة التأديب بأن الأدلة كافية لتقوم معها المخالفة التأديبيّة فلا تثريب عليها فيما توصلت إليه من قناعة حتى وإن خالفت الحكم القضائيّ الصادر بالبراءة.[24]

وأكدت ذلك المحكمة الإداريّة العليا المصريّة في أحد أحكامها؛ إذ قضت بأنه «متى ثبت أن الحكم الصادر من المحكمة الجنائيّة بتبرئة الموظّف لم يستند إلى عدم صحة الواقعة الجنائيّة، وإنما بني على الشك وعدم كفاية الأدلة، فهذا لا يرفع الشبهة نهائيًا، ولا يحول دون محاكمته تأديبيًا وإدانة سلوكه الإداريّ من أجل هذه التهمة عينها على الرغم من حكم البراءة»[25].

وكذلك استقرّ مجلس الدولة الفرنسيّ على أن الحكم الصادر بالبراءة لعدم كفاية الأدلة ليس له أي تأثير أمام قضاء التأديب، أما الحكم بالبراءة للشك فقد أبقى قضاء مجلس الدولة حرية التصرف لسلطة التأديب لاتخاذ ما تراه مناسبًا من إجراءات بحق الموظّف.[26]

(23) انظر: المجدلاوي، مخيمر يوسف، مرجع سابق، ص130. والكبيسي، مها خليفة راشد، أثر الحكم الجنائي على المسؤوليّة التأديبيّة للوظف العام في التشريع القطريّ: دراسة مقارنة، رسالة ماجستير، كلية القانون (جامعة قطر)، قطر، 2021، ص74

(24) المجدلاوي، مخيمر يوسف، مرجع سابق، ص130. الكبيسي، مها خليفة راشد، المرجع السابق، ص74.

(25) الطعن رقم 634 لسنة 3ق – تاريخ الجلسة 8-3-1985.

(26) نويجي، محمد فوزي، مرجع سابق، ص143.

وعلى الرغم من ندرة الأحكام القضائيّة في قطر بهذا الشأن إلا أنه بقياس النصوص القانونيّة في قطر وتشابهها إلى حد كبير مع نصوص القانون المصريّ، فيتضح لنا أن القضاء القطريّ سوف يكون موقفه مشابهًا لموقف القضاء المصريّ بهذه الحالة، فالأحكام القضائيّة الصادرة بالبراءة لعدم كفاية الأدلة لا تقيد سلطة الإدارة بمساءلة الموظّف تأديبيًّا، طالما اقتنعت هيئة التأديب بالأدلة المطروحة أمامها.[27]

ثانيًا: حكم البراءة المبني على بطلان الإجراءات:

من أهم المبادئ المستقر عليها في القانون الجنائيّ هو مبدأ حرية القاضي في الاقتناع، فيتمتع القاضي وفقًا لهذا المبدأ بحرية في قبول الدليل من عدمه وتقدير قيمته الثبوتية في الدعوى، إلا أن هذا المبدأ مقيد بوجوب استناد القاضي على أدلة مشروعة، فيلتزم القاضي بطرح كل دليل ثبت أن تحصيله تم بطريقة غير مشروعة، ومن ثم يقوم باستبعاده والحكم ببراءة المتهم لبطلان الإجراءات طالما كان هذا الدليل هو الدليل الوحيد لإدانة المتهم. إذن فإن الحكم بالبراءة لبطلان الإجراءات هو سبب إجرائيّ غير متعلق بموضوع الدعوى.[28]

ولم ينصّ القانون القطريّ وكذلك القانون المصريّ على حجيّة الحكم الجنائيّ الصادر بالبراءة على المساءلة التأديبيّة، كما أنّه لم يرد في الأحكام القضائيّة القطريّة ما يوضح موقف المشرع بهذا الشأن.

ويرى غالبية الفقه الإداريّ أن صدور حكم قضائيّ بالبراءة لعيب شكليّ في الإجراءات لا يحول دون مساءلة الموظّف تأديبيًّا وتوقيع العقوبة عليه لخروجه عن مقتضيات الوظيفة، فلا حجة لهذا الحكم أمام سلطات التأديب.[29]

أما بالنسبة للقضاء المصريّ فقد كان موقفه واضحًا بهذا الشأن إذ قضت المحكمة الإداريّة العليا المصريّة في أحد أحكامها بأن «متى ثبت أن المحكمة الجنائيّة قد قضت ببراءة المدعي من تهمة تعاطي المخدرات، وكان سبب البراءة يرجع إلى عيب شكليّ في إجراءات ضبط الواقعة، وهو بطلان التفتيش، بمقولة إن الحالة التي هوجم فيها المقهى لم تكن من حالات التلبس التي تسوغ قانونًا تفتيش المقهى، فإن هذا الحكم لا ينفي

(27) الكبيسي، مها خليفة راشد، مرجع سابق، ص74.

(28) زكي، محمد، الاثبات في المواد الجنائيّة محاولة فقهيّة وعملية لإرساء نظرية عامة، ب ط، الفنية للطباعة والنشر، الإسكندرية، 1985، ص-104 106.

(29) الجمعات، أكرم محمود، العلاقة بين الجريمة التأديبيّة والجريمة الجنائيّة، رسالة ماجستير، جامعة الشرق الأوسط (كلية الحقوق)، فلسطين، س2010. ص183

قيام سبب الجزاء التأديبي وهو إخلال الموظّف المتهم بواجبات وظيفته أو الخروج على مقتضياتها، وقد ثبت ذلك للسلطة التأديبيّة من أوراق التحقيقات الجنائيّة، .....، فإذا استفادت من ذلك كله أن المدعي أخل بواجبات وظيفته وخرج عن مقتضيات السلوك الواجب على رجل البوليس والابتعاد عمّا يحط من كرامته ويسيء سمعته فإن الجزاء التأديبي يكون قد قام سببه».[30]

ومثال على ذلك أن يدفع الموظّف أمام سلطات التأديب بالحكم الجنائيّ الصادر بالبراءة لبطلان التفتيش لتجاوز مأمور الضبط القضائيّ حدود التفتيش؛ ما أدى إلى العثور على مواد مخدرة ومحظورة قانونًا، وبطلان عينة الدم التي ظهرت نتيجتها إيجابية لاحتوائها على آثار تعاطي المواد المخدرة باعتبارها مبنية على التفتيش الباطل. وبناء على ما سبق بيانه من آراء القضاء والفقه، فإن سلطة التأديب لا تتقيد بما جاء في حكم البراءة من بطلان الإجراءات؛ إذ تكتفي بأن الأدلة المطروحة أمامها تثبت بأن المتهم قد سلك مسلكًا يناقض كرامة الوظيفة وحسن سمعتها، وارتكب فعلاً يعد خروجًا عن مقتضيات الواجبات الوظيفية.

ويرى جانب آخر من الفقه أن حكم البراءة المترتب على استبعاد الأدلة المتحصلة من إجراءات جوهرية باطلة، له حجيّة أمام سلطات التأديب، فليس لها أن تدين موظّفا بناء على أدلة حكمت المحكمة بعدم مشروعيتها، ومع ذلك ليس هناك ما يمنعها من مساءلة الموظّف إذا استندت في حكمها على أدلة لم تبطلها المحكمة أو لم تتصدّ لها.[31]

ثالثًا: حكم البراءة المؤسس على انعدام وجود الواقعة المادية:

قد يحصل أن يحكم القاضي الجنائيّ ببراءة المتهم لانتفاء الركن المادي للجريمة، كالموظّف الذي يتم اتهامه بجريمة اختلاس إلا أنّ الإدارة تعثر على المال محل الجريمة في الخزنة، فهنا تنتفي الواقعة المادية لجريمة الاختلاس، ويثار التساؤل حول مدى حجيّة الحكم الصادر بالبراءة في هذه الحالة على سلطة التأديب؟

يكاد الفقه الإداريّ أن يجمع على أن صدور حكم قضائيّ بالبراءة لانتفاء الركن المادي في الجريمة له حجيّة مطلقة أمام سلطات التأديب، فليس للسلطة التأديبيّة أن تعود وتنسب الفعل للموظّف وتوقع العقوبة عليه، وذلك لانعدام الأساس القانونيّ الذي من المفترض أن يرتكز عليه القرار التأديبي.[32]

(30) الطعن رقم 1655 لسنة 2ق – جلسة تاريخ 14-12-1957.

(31) الكبيسي، مها خليفة راشد، مرجع سابق، 76.

(32) ربيعة، بوقرط، حجيّة الحكم النهائي أمام سلطات التأديب الإداريّة بالجزائر، مجلة الاكاديمية للدراسات الاجتماعية

ويلاحظ أن المشرع القطريّ أقرّ بحجيّة الحكم الصادر بالبراءة لانتفاء الواقعة المادية أمام المحاكم المدنية، الأمر الذي يقرر له الحجيّة من باب أولى في المساءلة التأديبيّة لاستناد هذه الأخيرة على ذات الوقائع التي تستند إليها الدعوى الجنائيّة، وقد جاء في أحد أحكام محكمة التمييز القطريّة أن «الحكم الصادر في الدعوى الجنائيّة تكون له حجيّة في الدعوى المدنية، وهذه الحجيّة لا تقتصر على ركن الخطأ وحده وإنما تشمل- على مقتضى المادتين (319) من قانون الإجراءات الجنائيّة و (301) من قانون المرافعات المدنية-ما فصل فيه الحكم فصلاً لازمًا في وقوع الفعل المكون للأساس المشترك بين الدعويين الجنائيّة والمدنية وفي الوصف القانونيّ لهذا الفعل ونسبته إلى فاعله. فإذا فصلت المحكمة الجنائيّة في هذا الأمور فإنه يمتنع على المحاكم المدنية أن تعيد بحثها ويتعين عليها أن تلتزمها في بحث الحقوق المدنية المتصلة بها؛ لكيلا يكون حكمها مخالفًا للحكم الجنائيّ السابق له».[33]

ومع ذلك ليس هناك ما يمنع سلطة التأديب من مساءلة الموظّف إذا قدرت بأن سلوك الموظّف من الناحية التنظيمية لا يتفق مع القواعد العامة للسلوك الواجب، طالما أن حكمها تأسس على واقعة لم يفصل فيها الحكم الجنائيّ أو لم يعدم صحة وقوعها.[34]

رابعًا: صدور حكم البراءة لانعدام المسؤوليّة الجنائيّة:

يحدث أن تنتفي المسؤوليّة الجنائيّة بسبب وجود قوة قاهرة، أو فقدان الإدراك والتمييز بسبب عاهة عقلية، أو مرض نفسي، أو جنون، ويستوي كذلك أن يفقد الشخص عقله نتيجة تعاطيه للكحول أو المواد التي تذهب العقل بكامل إرادته.

ويرى الفقه أن انعدام المسؤوليّة الجنائيّة بسبب الجنون أو القوة القاهرة أو لأي سبب خارج عن إرادة المتهم يغلق باب المساءلة الجنائيّة، ومن ثم يغلق بالمقابل باب المساءلة التأديبيّة لانعدام الأهلية الجنائيّة وحرية الاختيار لدى المتهم عند وقوع الفعل، بينما يرفض رفع المسؤوليّة التأديبيّة عن الموظّف إذا كان فقدانه للاختيار والتمييز قد تم بإرادته مثل أن يكون تعاطى الكحول عمدًا ومن ثمّ أقدم على الجريمة، فلا يرى الفقه أن ذلك مانع من المسؤوليّة التأديبيّة كما أنه ليس مانعًا من المسؤوليّة الجنائيّة.[35]

والإنسانية، ع6، الجزائر، س 2011، ص89.

(33) محكمة التمييز القطريّة الطعن رقم 44 لسنة 2008 – جلسة تاريخ 27-5-2008

(34) نويجي، محمد فوزي، ص142.

(35) طلحة، نورة، مدى تبعية النظام التأديبي للموظّف العام للنظام الجزائي في النظام الجزائري، مجلة القانون العام الجزائري والمقارن، ع1، م5، الجزائر، 2019ص47.

وفي هذا الاتجاه ذهبت محكمة التمييز القطريّة في حكم لها «مناط الإعفاء من العقاب لفقدان الجاني شعوره وإدراكه وقت ارتكاب الفعل هو أن يكون السبب في هذه الحالة راجعًا على ما تقضي به المادة (54) من قانون العقوبات لجنون أو عاهة في العقل، أما سائر الأحوال النفسية التي لا تفقد الشخص الشعور والإدراك فلا تعد سببًا لانعدام المسؤوليّة، وكان المستفاد من دفاع الطاعن أمام المحكمة أنه يعاني من مرض نفسي، فإن الحكم المطعون فيه إذ انتهى على عدم تأثير ذلك على سلامة عقله وصحة إدراكه ورتب على ذلك مسؤوليته الجنائيّة عن الفعل الذي وقع منه يكون صحيحًا في القانون».[36]

وقضت في أحد أحكامها كذلك أن «المستفاد من نص المادة (54) من قانون العقوبات أن مناط انتفاء المسؤوليّة الجنائيّة في حالة السكر أن تكون المسكرات قد أعطيت له قسرًا عنه أو تناولها بغير علم منه وهو ما لا يدعيه الطاعن. ومن ثمّ فإن ما يثيره بدعوى انتفاء مسؤوليته عن التهمتين الثانية والثالثة- اللتين أثبتهما الحكم في حقه- لا يكون سديدًا».[37]

وقد تكون الأحكام القطريّة المتعلقة بإعفاء الموظّف من المسؤوليّة التأديبيّة بسبب انعدام الإدراك والاختيار لديه نادرة، إلا أنّ المحكمة الإداريّة العليا في مصر قد أصدرت حكمًا بهذا الشأن استندت فيه إلى ذات القواعد القانونيّة التي وردت في القانون القطريّ؛ حيث قضت أنه «فإذا ثبت صحة واقعتي التزوير والاختلاس المنسوبتين إلى المدعي ماديًا وقانونيًا، فإنّه لا يسأل عنهما بسبب المرض العقليّ الذي أصابه وقت وقوع هاتين الجريمتين، ومن ثمّ يتحقق انعدام سبب القرار التأديبي بفصل المدعي من الخدمة؛ وذلك لعدم جواز مساءلة الموظّف عن مرضه العقلي نظرًا للأثر الخطير لهذا المرض على سلوكه».[38]

خامسًا: تخلف أحد أركان الجريمة الجنائيّة:

قد تحكم المحكمة بالبراءة نتيجة انتفاء القصد الجنائيّ في الجرائم العمدية، وانتفاء الخطأ في الجرائم غير العمدية، ولا تنفي البراءة لهذه الأسباب حق الإدارة بمساءلة الموظّف تأديبيًا طالما أن المحكمة أقرت بصحة وجود الواقعة المادية، ومن ثمّ فلا يحول حكم البراءة دون مساءلة الموظّف تأديبيًا باعتبار أنّ الفعل يشكّل جريمة تأديبيّة.[39]

(36) محكمة التمييز القطريّة، جنائي، الطعن رقم 18 لسنة 2009 ق، بتاريخ 2-2-2009.

(37) محكمة التمييز القطريّة، جنائي، الطعن رقم 152 لسنة 2009 ق، بتاريخ 15-6-2009.

(38) قرار محكمة القضاء التأديبي المصريّة، جلسة 12 يناير 1978، دعوى 905، أورده العجاج، مصون طلال، أثر الحكم الجزائي على تأديب الموظّف العام، رسالة ماجستير، كلية القانون (جامعة اليرموك)، الأردن، 2015م، ص113

(39) نويجي، محمد فوزي، ص147

فقد تحكم المحكمة ببراءة المتهم من جريمة سرقة ممتلكات من جهة عمله، إلا أنه يساءل تأديبيًا عن إهماله وتقصيره في أداء عمله الذي تسبب بضياع تلك الممتلكات أو سرقتها.

ويعود ذلك إلى اختلاف النظام الجنائيّ عن النظام التأديبي في مناط تأثيم الفعل، ومبدأ الاستقلال بين الجريمة التأديبيّة والجريمة الجنائيّة، حيث يختلف التكييف الجنائيّ عن التكييف التأديبي، فينظر القضاء الجنائيّ إلى مدى توفر أركان الجريمة، بينما تنظر السلطة التأديبيّة إلى الواقعة بمدى اعتبارها خروجًا عن مقتضيات الواجبات الوظيفة التي يسبب الإخلال بها مساءلة تأديبيّة؛ ومن ثم يحق للسلطة التأديبيّة مساءلة الموظّف تأديبيًا وتوقيع العقوبة عليه طالما ليس هناك تعارض بين الحكم الجنائيّ بالبراءة والحكم التأديبي بخصوص ثبوت الفعل أو نفيه.[40]

ولم يرد في القانون والقضاء القطريّ ما ينظم هذه المسألة، وذلك بعكس القضاء المصريّ الذي قضى في أحد أحكامه أن «العجز في العهدة نتيجة تلاعب العامل الذي هو الأمين على العهدة أو نتيجة إهماله يمثل جريمة تأديبيّة يستحق عنها العامل الجزاء التأديبيّ، وذلك بغض النظر عما إذا كان هذا الفعل قد توفرت له أركان جريمة الاختلاس وفقًا لأحكام القانون الجنائيّ، وذلك لاختلاف مناط العقاب الجنائيّ عن العقاب التأديبي».[41]

وبالاستناد إلى القواعد العامة والآراء الفقهيّة يتبيّن لنا أنّ موقف القضاء القطريّ لن يكون مختلفًا عن موقف المحكمة الإداريّة العليا في مصر في حال عرضت عليه مسألة تتعلق بهذا الأمر، وذلك لكون القضاء سوف يستند إلى قواعد قانونيّة مشابهة للقواعد التي استندت إليها المحكمة العليا في مصر.

سادسًا: البراءة لشيوع التهمة:

قد تقضي المحكمة ببراءة المتهمين كافة في الجريمة لعدم تمكنها من تحديد الشخص المتهم من بين عدة متهمين، مع أن الثابت أن من ارتكب الجريمة شخص واحد فقط، بمعنى أن الجريمة شائعة بين عدة أشخاص.[42]

(40) الفايز، باسل محمد، أثر الحكم الجزائي على تأديب الموظّف العام، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2018م، ص85

(41) المحكمة الإداريّة العليا المصريّة، الطعن رقم 2998 لسنة 42 جلسة 8-8-1999.

(42) الجوهري، كمال عبد الواحد، قواعد المسؤولية التأديبيّة والجنائيّة والمدنية في مجال تأدية أعمال المحاماة بسبب مخالفة قانون المهنة والاخلال بواجباتها وتقاليدها والحط من قدرها دراسة تطبيقية في التشريع والقضاء في كل من مصر ودولة الكويت، ط١، المركز القومي للإصدارات القانونيّة، القاهرة، 2015، ص412.

ومثال على ذلك أن يقرر بعض الموظّفين الذين يعملون في إحدى مؤسسات الدولة السفر معًا ويقومون بوضع أغراضهم في حقيبة واحدة، وعند تفتيش الحقيبة في المطار يتم العثور على لفافة تحتوي على مواد مخدرة، وعند إحالة المتهمين إلى النيابة العامة ينكر جميعهم التهم المنسوبة إليهم، ولا تتمكن المحكمة من تحديد صاحب المواد المخدرة، وعليه تقضي ببراءتهم جميعًا لشيوع التهمة.

ويثور التساؤل في هذه الحالة حول مدى أحقية الجهة الإداريّة بمجازاة موظّفيها تأديبيًا رغم صدور حكم بالبراءة لشيوع التهمة؟

إن القاعدة المستقر عليها في مجال المسؤوليّة التأديبيّة والمسؤوليّة الجنائيّة والتي أكدتها الدساتير هي شخصية العقوبة، أي أنه لا يجوز إنزال العقوبة إلا على من ارتكب الفعل وثبتت مسؤوليته عنه، فلا يسأل الشخص إلا عن الأفعال التي تصدر منه دون غيره،[43] ويجد هذا المبدأ مدلوله في أحكام الشريعة الإسلامية لقوله تعالى: (قُلْ أَغَيْرَ اللَّهِ أَبْغِي رَبًّا وَهُوَ رَبُّ كُلِّ شَيْءٍ وَلَا تَكْسِبُ كُلُّ نَفْسٍ إِلَّا عَلَيْهَا وَلَا تَزِرُ وَازِرَةٌ وِزْرَ أُخْرَى ثُمَّ إِلَى رَبِّكُمْ مَرْجِعُكُمْ فَيُنَبِّئُكُمْ بِمَا كُنْتُمْ فِيهِ تَخْتَلِفُونَ).[44]

واستنادًا على ذلك فإن شيوع التهمة يعد سببًا للبراءة في الدعوى التأديبيّة مثلما يّعد سببًا للبراءة في الدعوى الجنائيّة، وذلك لانعدام اليقين في تحديد مرتكب الفعل الذي شكل المخالفة التأديبيّة، إذ إنّه لا يُسأل تأديبيًا إلا من ثبت ارتكابه لفعل سلبيّ أو إيجابيّ يخالف مقتضيات وواجبات وظيفته.[45]

وتطبيقًا لذلك قضت المحكمة الإداريّة العليا في مصر بأنّه يتعين لإدانة الموظّف ومجازاته تأديبيًا في حالة شيوع التهمة أن تثبت الإدارة أنّه قد وقع منه فعل إيجابيّ أو سلبيّ محدد يعد مساهمة في وقوع المخالفة الإداريّة التي سوغت ارتكاب الواقعة الجنائيّة المجهول فاعلها. وفي حال أثبتت الإدارة مساهمة الموظّف فإن البراءة من العقوبة الجنائيّة بسبب شيوع التهمة لا تكون سببًا مانعًا من المساءلة التأديبيّة. أما إذا تعذر إثبات ذلك فلا يكون ثمة ذنب إداريّ يمكن توجيهه للموظّف، ومن ثمّ لا محل لتوقيع الجزاء التأديبيّ عليه.[46]

(43) المادة 40 من الدستور الدائم لدولة قطر.

(44) القرآن الكريم، سورة الأنعام، الآية (164).

(45) الجوهري، كمال عبد الواحد، مرجع سابق، ص413.

(46) المحكمة الإداريّة العليا، إداريّ، الطعن رقم (25024)، لسنة 59 ق.

الفرع الثاني: حجيّة الحكم الجنائيّ الصادر بالإدانة على سلطات التأديب

من المعلوم أن صدور الحكم الجنائيّ بالإدانة لا بد أن يقوم على الجزم واليقين والدليل القاطع، فإنّ وجد القاضي أنّ الوقائع التي ثبتت صحتها ونسبتها إلى المتهم تشكل جريمة جنائيّة فيحكم على الفور بالإدانة، وبمجرد صدور الحكم فإنه يكتسب الحجيّة التي تدل دلالة قاطعة أن الفعل الذي يشكل جريمة جنائيّة ومخالفة تأديبيّة قد وقع من قِبل المتهم ذاته.[47]

وقد أجمع الفقه والقضاء بأن الأحكام الجنائيّة الصادرة بالإدانة لها حجيّة مطلقة أمام سلطات التأديب، فلا يجوز لسلطة التأديب بأي حال من الأحوال أن تحكم بخلاف ما جاء في الحكم القضائيّ أو تعاود البحث بصحة الواقعة ونسبتها إلى المتهم، ذلك أنه من غير المعقول إثبات الفعل المكون للجريمة ونسبته إلى المتهم أمام المحاكم الجنائيّة، وتبرئة المتهم منه أمام المحاكم التأديبيّة.[48]

وقد خلا القانون القطريّ وكذلك القانون المصريّ من نص يعطي الحكم الجنائيّ الصادر بالإدانة الحجيّة المطلقة أمام سلطات التأديب، إلا أن نص المادتين (319) من قانون الإجراءات القطريّ و(456) من قانون الإجراءات المصريّ. جاء حسب رأي الفقه والقضاء بمعنى واسع وكافٍ ليشمل الحجيّة أمام المحاكم المدنية وأمام سلطات التأديب.[49]

ومن جانبنا لا نرى أن هاتين المادتين كافيتان لمعالجة حجيّة الحكم الجنائيّ أمام سلطات التأديب ذلك لما بين الدعوى المدنية والدعوى التأديبيّة من اختلاف، علاوة على اختلاف علاقة كل منهما بالدعوى الجنائيّة.

أما فيما يتعلق بموقف القضاء المصريّ فقد أكد حجيّة الحكم الجنائيّ الصادر بالإدانة أمام سلطات التأديب، فذهبت المحكمة الإداريّة العليا في أحد أحكامها إلى «إن الأحكام الجنائيّة التي حازت قوة الأمر المقضي به تكون حجة فيما فصلت فيه، ويعتبر الحكم عنوان الحقيقة فيما قضى به، والذي يحوز الحجيّة من الحكم هو منطوقه والأسباب الجوهرية المكملة له، والقضاء التأديبي يرتبط بالحكم الجنائيّ في الوقائع التي فصل فيها، إذا شكل الفعل في ذات الوقت مخالفة إداريّة، وبالتالي يعتبر الحكم حجيّة فيما فصل فيه، ولا تعاود المحكمة التأديبيّة المجادلة في إثبات الوقائع التي سبق لحكم جنائيّ حاز قوة الأمر المقضي به أثبت وقوعها».[50]

(47) العجاج، مصون طلال محمد، مرجع سابق، ص45.

(48) طلحة، نورة، مرجع سابق، ص47.

(49) نويجي، محمد فوزي، مرجع سابق، ص117 118-.

(50) المحكمة الإداريّة العليا، الطعن رقم 7688 لسنة 46 ق، جلسة 30-3-2002.

ويلاحظ أن الأحكام الجنائيّة الصادرة بالإدانة ليست على شاكلة واحدة، فبعضها يؤدي إلى وجوب إنهاء الدعوى التأديبيّة لانتهاء الرابطة الوظيفية بين الموظّف والإدارة بقوة القانون، والبعض الآخر من الأحكام لا تلزم الإدارة سوى بإدانة الموظّف وتترك لها سلطة اختيار العقوبة المناسبة للفعل الذي ارتكبه الموظّف، وقد تم تخصيص هذا الفرع لبيان آثار هذه الأنواع.

أولًا: الحكم الجنائيّ الصادر بالإدانة الذي ينهي الرابطة الوظيفية بين الموظّف والإدارة بقوة القانون:

سبق وأن بينا أن التشريعات المنظمة للوظيفة العامة لم تتطرق إلى حجيّة الحكم الجنائيّ أمام سلطات التأديب كما فعلت بشأن حجيته أمام المحاكم المدنية، ومع ذلك فإن بعض الأحكام الجنائيّة حين تصدر تلحق بالعقوبة الأصلية عقوبة تبعية بقوة القانون تقضي بفصل الموظّف من وظيفته، دون أن تترك للإدارة سلطة اختيار عقوبة أخرى، وقد ورد هذا الحكم بشكل صريح في نص المادة (7\107) من قانون الموارد البشرية القطريّ والتي جاء فيها أن خدمة الموظّف تنتهي في عدة حالات ومن ضمنها «صدور حكم نهائي ضده في جريمة مخلة بالشرف أو الأمانة، ومع ذلك فإذا كان الحكم مشمولاً بوقف تنفيذ العقوبة، أو كان لأول مرة فلا يترتب عليه إنهاء الخدمة إلا إذا قدرت الجهة الحكومية بقرار مسبب من واقع أسباب الحكم وظروف الواقعة أن بقاء الموظّف يتعارض مع مقتضيات الوظيفة أو طبيعة العمل».

ويثار التساؤل حول أثر هذا الفصل على السلطة التأديبيّة، فهل عليها إنهاء الدعوى التأديبيّة لكون الفصل بمثابة جزاء تأديبي يتم بقوة القانون، أم لها الاستمرار في الدعوى وتوقيع عقوبة مختلفة على الموظّف باعتبار أن الفصل في هذه الحالة لا يعد جزاءً تأديبيًّا؟

يذهب جانب من الفقه إلى أن الفصل كعقوبة تبعية للعقوبة الجنائيّة الأصلية لا يعد جزاءً تأديبيًّا، ومن ثمّ ليس هناك ما يمنع سلطة التأديب من الاستمرار في الدعوى التأديبيّة وتوقيع عقوبة مختلفة على الموظّف دون أن يكون هذا إخلالاً بمبدأ عدم تعدد العقوبات على الفعل الواحد.[51]

بينما يرى الجانب الآخر – وهو الراجح – أنّ الفصل من الوظيفة يبقى جزاءً تأديبيًّا، ولا يغير من طبيعته صدوره كعقوبة تبعية من المحكمة الجنائيّة؛ إذ إن الفصل عقوبة تصيب

(51) ربيعة، بوقرط، مرجع سابق، ص88.

الـموظّف فـي حياته الوظيفـية شـأنه شـأن الجزاءات التأديبيّة الأخرى، ومن ثمّ فلا يجوز لسـلطة التأديب أن تحكم بعقوبـة تأديبيّـة أخـرى لـما فـي ذلـك مـن تكـرار محظـور للعقـاب التأديبـي.[52]

ومـن جانبنـا نتفـق مـع الـرأي الثانـي الـذي يـرى أن الفصـل يبقـى جـزاءً تأديبيًـا سـواء أوقعتـه السـلطة التأديبيّـة أم تم بقـوة القانـون؛ إذ إن سـلطة التأديـب تلتـزم بإنهـاء الدعـوى التأديبيّـة بمجـرد صـدور الحكم النهائـي؛ ذلـك لأن الفصـل أقسـى الجـزاءات التأديبيّـة التـي يمكـن توقيعهـا علـى الـموظّف، وبموجبـه يفقـد الـموظّف صفتـه التـي يجـب توفرهـا عنـد الـمساءلة التأديبيّـة، ومـن ثمّ أي عقوبـة تأديبيّـة أخـرى لـن تكـون مجديـة بحـق الـموظّف، فليـس هنـاك محـل للخصـم مـن راتبـه أو تخفـيض درجتـه أو توقيـع أي عقوبـة أخـرى عليـه؛ ذلـك لأن هـذه العقوبـات كافـة تسـتلزم أن يكـون الـموظّف علـى رأس عملـه لكـي يتـم تنفـيذها، وفصـل الـموظّف ينهـي الصلـة الوظيفـية بين الـموظّف والإدارة، وتمحـى كل الحقـوق والواجبـات الـمتبادلة بين الطرفـين، ومـن ثم يسـتحيل تنفـيذ العقوبـة عليـه.

وبالعـودة إلـى نـص الـمادة (107) يلاحـظ أنهـا قـررت شـرطًا أساسـيًا بالإضافـة إلـى الشـروط العامـة لحجيّـة الحكـم الجنائـيّ -والتـي سـبق ذكرهـا فـي الـمطلب الأول- لكـي تنتهـي خدمـة الـموظّف بعقوبـة تبعيـة، ويتمثـل هـذا الشـرط فـي أن يكـون الحكـم الجنائـيّ صـادرًا بجريمـة ماسـة بالشـرف أو الأمانـة، ويلاحـظ مـن نـص الـمادة (107) أن الـمشرع القطـريّ اكتفـى بـأن تكـون الجريمـة التـي أديـن بهـا الـموظّف بحكـم نهائـي مـن جرائـم الشـرف والأمانـة، وهـذا بعكـس موقـف الـمشرع الـمصريّ الـذي اشـترط فـي نـص الـمادة (69) مـن قانـون الخدمـة الـمدنية أن تكـون الجريمـة التـي أديـن بهـا الـموظّف مـن جرائـم الجنايـات أو جريمـة مقيـدة للحريـة مـن جرائـم الشـرف والأمانـة.[53]

ولـم يحدد الـمشرع القطريّ العقوبات الـماسة بالشـرف والأمانة، وترك الأمر للفقه والقضاء، وقـد جـاء فـي فتـوى لإدارة الفتـوى والعقـود فـي قطـر إلـى أن «حيـث إنـه ولئـن كانـت الجرائـم الـمخلة بالشـرف أو الأمانـة غيـر محـددة فـي قانـون العقوبـات أو أي قانـون أخـر تحديـدًا جامعًـا مانعًـا، إلا أن مـن الـمستقر عليـه فقهًـا وقضـاءً يمكـن تعريـف هـذا الجرائـم بأنهـا هـي تلـك التـي ترجـع إلـى ضعـف فـي الخلـق وانحـراف فـي الطبـع مـع الأخـذ فـي الاعتبـار طبيعـة الوظيفـة ونـوع العمـل الـذي يؤديـه العامـل الـمحكوم عليـه، ونـوع الجريمـة والظـروف التـي ارتكبـت فـيها، والأفعـال الـمكونة لهـا، ومـدى كشـفها عـن التأثـر بالشـهوات، والنـزوات، وسـوء السـيرة، ممـا

(52) عواملـه، عمـر سـلمان محمـد، حجيّـة الحكـم الجنائي أمـام سـلطات التأديـب- دراسـة مقارنـة بين مصـر والأردن، رسـالة دكتـوراة (جامعـة العلـوم الإسـلامية العالـمية)، الأردن، س2014، ص182

(53) قانون الخدمة المدنية رقم المصريّ، رقم 81 لسنة 2016.

ينعكس أثر ذلك على العمل، وغير ذلك من الاعتبارات».[54] ومثال على الجرائم الماسة بالشرف والأمانة، جرائم الإضرار بالمال العام كالرشوة والاختلاس، الجرائم الواقعة على العرض، كالاغتصاب والزنا وهتك العرض.

ومع ذلك فقد قرر المشرع القطريّ حالتين لا تنتهي بهما خدمة الموظّف بقوة القانون وإن كان قد أدين بحكم نهائي في جريمة مخلة بالشرف والأمانة وهما:

- إذا كان الحكم مشمولاً بوقف التنفيذ.
- إذا كان الحكم صدر لأول مرة على الموظّف العام.

واستثنت المادة من يرتكب الفعل لأول مرة، ومن يكن حكمه مشمولاً بوقف التنفيذ من الفصل من الوظيفة بقوة القانون في الجرائم المخلة بالشرف والأمانة، وجعلت الحكم يقتصر على من كرر الجريمة لأكثر من مرة -العود- ومن كان حكمه نافذًا، وقد أعطى المشرع القطريّ الموظّف بموجب هذا الاستثناء فرصة للاتعاظ واتباع السلوك الحميد وعدم العودة إلى الفعل الذي يؤدي إلى فصله من الوظيفة[55].

في حين أن المشرع المصريّ لم يورد هذه الاستثناءات أو غيرها في نص المادة (69) من قانون الخدمة المدنية، إذ اكتفى بالنص على انتهاء خدمة الموظّف عند الحكم عليه بعقوبة جناية أو عقوبة مقيدة للحرية في جريمة مخلة بالشرف أو الأمانة أو تفقده الثقة والاعتبار.

ومع ذلك وإن تحققت الاستثناءات التي أوردها المشرع القطريّ في المادة السابق ذكرها إلا أنه ليس هناك ما يمنع الإدارة من انهاء خدمة الموظّف بقرار تأديبي إذا رأت أن الفعل الذي ارتكبه لا يتناسب مع بقائه في الوظيفة العامة[56]، بل وتلتزم بموجب الحكم الجنائيّ الصادر بالإدانة بالاستمرار في الدعوى التأديبيّة وتوقيع جزاء تأديبي على الموظّف يتناسب مع المخالفة المنسوبة إليه سواء كان الفصل من الوظيفة أم أي جزاء آخر.

ثانيًا: الحكم الجنائيّ الصادر بالإدانة الذي لا يؤثر على الرابطة الوظيفية بين الموظّف والإدارة

قد يصدر الحكم الجنائيّ بالإدانة بجرائم غير مخلة بالشرف والأمانة وذلك هو الغالب في المجال التأديبي وبالتالي لا يؤثر على الرابطة الوظيفية بين الموظّف والإدارة، وهذا النوع من الأحكام يترك الأمر لسلطة الإدارة التقديرية لتوقيع العقوبة التأديبيّة المناسبة على الموظّف وفقًا لجسامة المخالفة المرتكبة.

(54) إدارة الفتاوى والعقود في قطر، (ف.ع 3/-11 1535/ 2003، أورده: المحاسنة، فاطمة علي خليل، انتهاء خدمة الموظّف العام بقوة القانون في قانون الموارد البشرية المدنية القطريّ رقم 15 لسنة 2016 ولائحته التنفيذية بقرار مجلس الوزراء رقم 32 لسنة 2016، رسالة ماجستير، كلية القانون (قطر: جامعة قطر، س2021م)، ص62

(55) المحاسنة، فاطمة علي خليل، مرجع سابق، ص65.

(56) المادة (70\7) قانون المواد البشرية رقم (15) لسنة 2016.

والتزام السلطة التأديبيّة في هذه الحالة يكون بمنطوق الحكم والأسباب الجوهرية التي أدت إلى صدوره، أما بقية الحكم فللسلطة التأديبيّة أن تأخذ فيه على سبيل الاستئناس به في حكمها، فتراعي عند تقدير العقوبة الأسباب التي أدت إلى تشديد أو تخفيف العقوبة الجنائيّة وسوابق المتهم، وتقرر بناء عليه العقوبة التأديبيّة المناسبة وفقًا لتقديرها بمدى اعتبار الفعل خروجًا عن مقتضيات الواجب الوظيفي واخلالاً بكرامتها وبالسلوك القويم الذي يجب أن يراعى للحفاظ على حسن السيرة والأخلاق.[57]

ولا يجوز للإدارة عند استخدام سلطتها التقديرية أن تبرئ المتهم من المخالفة التأديبيّة في حال كان محل الدعوى التأديبيّة هو ذاته محل الدعوى الجنائيّة التي صدر فيها حكم بالإدانة.

وأكد القضاء الإداريّ التزام الإدارة بتوقيع العقوبة على المتهم في هذه الحالة، فذهبت المحكمة الإداريّة العليا المصريّة في أحد أحكامها إلى أنه «ومن حيث أن القضاء الجنائيّ هو المختص بإثبات أو نفي المسؤوليّة الجنائيّة عما وقع من المطعون ضده من أفعال تكون الجريمة الجنائيّة وقد قضى فيها بحكم نهائي حائز لقوة الأمر المقضي به فلا يسوغ للمحكمة التأديبيّة وهي بصدد محاكمته تأديبيًا عن ذات الأفعال في شقها التأديبي أن تعاود البحث في ثبوت أو عدم ثبوت هذه الوقائع في حق المطعون ضده أو مدى مسؤوليته عنها رغم وقوعها منه؛ لأن ذلك يتناقض مع حجيّة الحكم الجنائيّ الذي فصل في هذه المسألة بصفة نهائية وكان يتعين على المحكمة التأديبيّة أن تتقيد بما ورد بشأنها في الحكم الجنائيّ وإذا خلصت المحكمة التأديبيّة إلى براءة المطعون ضده تأسيسًا على عدم مسؤوليته عن هذه الأفعال استنادًا إلى أنه مصاب بأمراض عصبية ونفسية وأن ارتكابه للمخالفات كان في فترة مرضه فإنها تكون قد أخطأت في تطبيق القانون ويتعين لذلك إلغاء الحكم المطعون فيه».[58]

ويتضح أن الفقه عندما ألزم السلطات التأديبيّة بالتقيد بحكم الجنائيّ الصادر بالإدانة كان بغرض الأخذ بعدة اعتبارات، منها الاعتبارات القانونيّة، والاعتبارات العملية، وأخيرًا اعتبارات الأمر الواقع، وسوف نبين كلاً منها كالتالي:

- الاعتبارات القانونيّة: يعد الحكم الجنائيّ البات عنوانًا للحقيقة فيما توصل إليه أمام الكافة، فهو حجة بكل ما ورد فيه، خاصة فيما يتعلق بثبوت التهمة ونسبتها إلى فاعلها، والسماح

(57) د. هنداوي، السيد فتوح محمد، مرجع سابق، ص282-283.

(58) الطعن رقم 2495 لسنة 30 قضائيّة- بتاريخ 17-06-1986.

لسلطات التأديب بمعاودة البحث حول صحة ما ورد في الحكم الجنائيّ وإثبات عكس ما توصل إليه يؤدي إلى إضعاف قوته والتشكيك في مصداقيته.[59]

- الاعتبارات العملية: تعد المحكمة الجنائيّة هي صاحبة الاختصاص الأصيل بالبحث عن وقوع الجريمة ونسبتها إلى فاعلها، وهي بذلك تمتلك العديد من الصلاحيات والسلطات في الإثبات والتي تضمن الوصول إلى الحقيقة وهو ما لا تمتلكها السلطات التأديبيّة، كما أن المسائل الجنائيّة من المسائل المتعلقة بالنظام العام، ولا يتحقق الاستقرار إذا تم إصدار حكم من المحكمة الجنائيّة متعلقة بحق المجتمع في العقاب، ومن ثم قام قضاء محكمة أخرى بنقضه ومس أساسه وأركانه.[60]
- اعتبارات الأمر الواقع: يلاحظ تأثر النظام التأديبي إلى حد كبير مع النظام الجنائيّ من حيث المبادئ العامة، كالإجراءات والضمانات والآثار، وهذا التشابه هو ما يدعو إلى التزام السلطات التأديبيّة بحجيّة الحكم الجنائيّ واحترام النتيجة التي توصل إليها باعتبارها هي الحقيقة.[61]

(59) غنام، طارق فيصل مصطفى، مرجع سابق، ص104.

(60) نويجي، محمد فوزي، مرجع سابق، ص122.

(61) انظر: غنام، طارق فيصل مصطفى، مرجع سابق، ص105. نويجي، محمد فوزي، المرجع السابق، ص122.

الخاتمة:

تناول هذا البحث أثر حجيّة الحكم الجنائيّ على المساءلة التأديبيّة في القانون القطريّ في ضوء القانون المصريّ، وتم بيان أثر الحكم بحالتيه سواء صدر بالإدانة أم بالبراءة بكافة أسبابها. وتطرق البحث قبل ذلك إلى مفهوم حجيّة الحكم الجنائيّ، وأهم الشروط التي يجب قيامها لتمتع الحكم الجنائيّ بالحجيّة أمام سلطات التأديب، وعند التعمق في موضوع البحث وهو أثر حجيّة الحكم الجنائيّ على المساءلة التأديبيّة، انتهى إلى أن الحكم الجنائيّ الصادر بالإدانة له حجيّة مطلقة أمام سلطات التأديب، وسواء كان الحكم الصادر بالإدانة ينهي خدمة الموظّف بقوة القانون كعقوبة تبعية، أم يترك لسلطة التأديب حرية اختيار العقوبة، فإن كلتا الحالتين تقيد سلطات التأديب من حيث صحة الوقائع التي تشكل جريمة ونسبتها إلى المتهم، فليس للسلطة التأديبيّة وهي في طريقها للكشف عن تحقق المخالفة أن تحكم بخلاف ما قضى به الحكم الجنائيّ من صحة الوقائع المادية ونسبتها إلى الموظّف المتهم. بينما يثار الجدل الفقهيّ حول الحكم الصادر بالبراءة والتي تتعدد حالاته.

وبعد استعراض الآراء الفقهيّة المختلفة توصل البحث إلى أن ليست جميع أحكام البراءة تحوز الحجيّة أمام سلطات التأديب، فمنها ما له حجيّة أمام سلطات التأديب كالبراءة لعدم صحة الوقائع أو لانعدام المسؤوليّة الجنائيّة، فلا يجوز في هاتين الحالتين أن تعاود سلطة التأديب التحقيق في وجود أو نفي ما قرره حكم البراءة، فبالتالي لا محل لملاحقة الموظّف تأديبيًا. بينما بقية الحالات كالبراءة المبنية على عدم كفاية الأدلة، أو بطلان الإجراءات الجنائيّة، أو انعدام ركن من أركان الجريمة، أو شيوع التهمة فلا تمنع سلطة التأديب من ملاحقة الموظّف تأديبيًا، ولها مطلق الحرية في تقدير مسؤوليّة الموظّف التأديبيّة. وتوصل البحث إلى بعض النتائج والتوصيات نسردها فيما يلي

النتائج:

- لم يول القضاء القطريّ الاهتمام الكافي للمسائل المختلفة المتعلقة بحجيّة الحكم الجنائيّ أمام سلطات التأديب، في حين كان للقضاء المصريّ جهود واضحة في محاولة إرساء بعض القواعد القضائيّة التي تسهم في سد الخلل في ظل غياب النص القانونيّ الذي ينظم هذه المسائل.
- لحجيّة الحكم الجنائيّ أثران الأول سلبي يمنع كل محكمة أو جهة قضائيّة أخرى من إعادة النظر في الواقعة التي فصل فيها الحكم الجنائيّ، والآخر إيجابي يتمثل في افتراض الحقيقة فيما قضى به الحكم وانتهاء الدعوى الجنائيّة بكل عناصرها الشخصية والموضوعية.

- حتى يتمتع الحكم الجنائيّ بالحجيّة أمام سلطات التأديب لا بد من أن تتوافر فيه عدة شروط وانتفاء أحد هذه الشروط يفقد الحكم حجيته.
- لم يتصد المشرع القطريّ لحجيّة الحكم الجنائيّ أمام سلطات التأديب، ولا يمكن قياسه بشكل تام على المادة (319) لاختلاف طبيعة الدعوى التأديبيّة عن الدعوى المدنية وعلاقة كل منهما بالدعوى الجنائيّة.
- لا تتمتع كافة الأحكام الجنائيّة الصادرة بالبراءة بالحجيّة أمام سلطات التأديب، فبراءة الموظّف من الجريمة الجنائيّة لا تعني عدم مسؤوليته التأديبيّة، فذهب غالبية الفقه إلى أن الحكم بالبراءة لعدم كفاية الأدلة أو لبطلان الإجراءات الجنائيّة أو لانعدام ركن من أركان الجريمة أو لشيوع التهمة لا يحول دون ملاحقة الموظّف تأديبيًا طالما كان الفعل يشكل خروجًا عن مقتضيات الوظيفة.
- للحكم الجنائيّ الصادر بالإدانة حجيّة مطلقة أمام سلطات التأديب بإجماع من الفقه، فلا يجوز للسلطة التأديبيّة وهي بصدد مساءلة المتهم تأديبيًا أن تعاود البحث في صحة الوقائع المادية ونسبتها إلى المتهم.
- تقسم الأحكام الجنائيّة الصادرة بالإدانة إلى أحكام تؤثر على الرابطة الوظيفية بين الموظّف والإدارة وتسلب من الإدارة سلطة اختيار العقوبة، وأحكام لا تؤثر على الرابطة الوظيفية وتظل الإدارة محتفظة بحقها في اختيار العقوبة المناسبة للمخالفة المرتكبة.
- يذهب غالبية الفقه إلى أن فصل الموظّف بقوة القانون عند إدانته بجريمة مخلة بالشرف والأمانة يظل جزاءً تأديبيًا، ولا يغير من طبيعته صدوره كعقوبة تبعية للعقوبة الأصلية، ومن ثم تلتزم السلطة التأديبيّة بإنهاء خدمة الموظّف فورًا، وعدم تطبيق عقوبة أخرى عليه لما في ذلك من إخلال بمبدأ عدم معاقبة الشخص على الفعل مرتين.
- تقوم حجيّة الحكم الجنائيّ الصادر بالإدانة على عدة اعتبارات متمثلة في اعتبارات قانونيّة، واعتبارات عملية، واعتبارات الأمر الواقع.

التوصيات:

- يوصي البحث القضاء القطريّ بأن يبذل المزيد من العناية والجهد لإرساء القواعد القضائيّة التي تسهم في سد ثغرة عدم وجود نص قانونيّ ينظم مسألة حجيّة الحكم الجنائيّ على المساءلة التأديبيّة أسوة بالقضاء المصريّ.
- يقترح البحث على المشرع القطريّ بإعادة النظر في نص المادة (105) من قانون الموارد البشرية رقم (15) لسنة 2006، ليعطي سلطة تقديرية لجهة التأديب في وقف الدعوى التأديبيّة حتى يصدر الحكم الجنائيّ أسوة بقانون الخدمة العسكرية رقم (31) لسنة 2006، فليست جميع الحالات تستدعي إيقاف إجراءات الدعوى التأديبيّة، خاصة حين يكون لدى

جهة الإدارة أدلة كافية تثبت صحة الواقعة ونسبتها إلى المتهم. ونقترح أن يصبح النص كالتالي: (في الحالات التي تقرر فيها إحالة الموظّف إلى المحاكمة الجنائيّة، للسلطة المختصة أن توقف الإجراءات التأديبيّة إلى أن يصدر حكم نهائي من المحكمة المختصة).

- ضرورة تصدي المشرع القطريّ لحجيّة الأحكام الجنائيّة أمام سلطات التأديب وتخصيص مادة قانونيّة تنظم ذلك، ليسهم ذلك بتحديد الوضع القانونيّ للموظّف المخالف، وعدم ترك الأمر للاجتهادات القضائيّة والفقهيّة؛ إذ إنه من المستحيل أن تستقر هذه الاجتهادات على رأي محدد.
- يقترح البحث إضافة فقرة إلى نص المادة (7/70) من قانون الموارد البشرية، بحيث تنتهي خدمة الموظّف بقوة القانون عند صدور حكم جنائيّ عليه للمرة الثانية بجرائم المخدرات، باعتبارها من الجرائم التي أخرجها الفقهاء من إطار جرائم الشرف والأمانة، وباعتبارها من الجرائم شديدة الخطورة والتي تؤثر بشكل مباشر على سمعة الوظيفة لما فيها من انحراف شديد عن السلوك القويم الذي يجب على الموظّف العام أن يتحلى به.
- ضرورة أخذ السلطات التأديبيّة بعين الاعتبار الحكم الجنائيّ الصادر بالبراءة أو بوقف التنفيذ عند تقديرها للعقوبة.
- إلزام الإدارة عند مساءلة الموظّف تأديبيًا أن تسبب في حكمها بوضوح مدى تأثير فعل الموظّف الذي يشكل جريمة جنائيّة على الوظيفة العامة، ذلك أنه من غير المنطقي أن تتم مساءلة الموظّف على فعل لا يمت للوظيفة بصلة ولا يؤثر عليها على الاطلاق سواء بشكل مباشر أم غير مباشر.

قائمة المراجع:

الكتب:

- ابن منظور، لسان العرب، المجلد الثالث (ح)، ج3، الطبعة الثانية، دار إحياء التراث العربي، بيروت- لبنان، 1993.
- ثروت، جلال، د. عبد المنعم، سليمان، أصول المحاكمات الجزائية – الدعوى الجنائيّة، المؤسسة الجامعية للدراسات والنشر والتوزيع، ط1، 1996م.
- السنهوري، عبد الرزاق أحمد، الوسيط في شرح القانون المدني الجديد، نظرية الالتزام بوجه عام، الإثبات- آثار الالتزام، ج2، منشورات الحلبي الحقوقية (بيروت- لبنان)، 2010.

البحوث والرسائل:

- بوقرط، ربيعة، حجيّة الحكم النهائي أمام سلطات التأديب الإداريّة بالجزائر، بحث محكم، الأكاديمية للدراسات الاجتماعية والإنسانية، العدد (6)، الجزائر، سنة 2011.
- الجمعات، أكرم محمود، العلاقة بين الجريمة التأديبيّة والجريمة الجنائيّة، رسالة ماجستير، جامعة الشرق الأوسط (كلية الحقوق)، فلسطين، 2010.
- طلحة، نورة، مدى تبعية النظام التأديبي للموظّف العام للنظام الجزائي في النظام الجزائري، مجلة القانون العام الجزائري والمقارن، م5، ع1، الجزائر، 2019.
- العجاج، مصون طلال، أثر الحكم الجزائي على تأديب الموظّف العام، رسالة ماجستير، كلية القانون (جامعة اليرموك)، الأردن، 2015م.
- عنيبة، علي محمد علي، حجيّة الحكم الجنائيّ أمام القضاء المدني، مجلة البحوث القانونيّة، المجلد الثالث، العدد الثاني، ليبيا، أبريل 2016م.
- عوامله، عمر سلمان محمد، حجيّة الحكم الجنائيّ أمام سلطات التأديب- دراسة مقارنة بين مصر والأردن، رسالة دكتوراه (جامعة العلوم الإسلامية العالمية)، الأردن، 2014.
- غنام، طارق فيصل، العلاقة بين الجريمة التأديبيّة والجريمة الجنائيّة: دراسة مقارنة، رسالة ماجستير، كلية الدراسات العليا (جامعة النجاح الوطنية)، فلسطين، 2016.
- الكبيسي، مها خليفة راشد، أثر الحكم الجنائيّ على المسؤوليّة التأديبيّة للوظف العام في التشريع القطريّ: دراسة مقارنة، رسالة ماجستير، كلية القانون (جامعة قطر)، قطر، 2021.
- المجدلاوي، مخيمر يوسف، حجيّة القرارات والأحكام الجزائية في المجال التأديبي، دراسة مقارنة بين القانونيّن المصريّ والفلسطيني، رسالة ماجستير، كلية الحقوق (جامعة الأزهر)، غزة، يوليو 2013.

- نويجي، محمد فوزي، حجيّة الأحكام الجنائيّة على الجريمة التأديبيّة في ضوء القانون القطريّ، المجلة القانونيّة والقضائيّة، ع1، قطر، 2021.
- هنداوي، السيد فتوح محمد، أثر الحكم الجنائيّ على المسؤوليّة التأديبيّة للموظّف العام في النظام القانونيّ السعودي، مجلة البحوث الاقتصادية والقانونيّة، ع24، مصر، 2020.

الأحكام القضائيّة والفتاوى:

الأحكام القطريّة:

- محكمة التمييز القطريّة الطعن رقم 202 لسنة 2013 ق، جلسة 18-11-2013.
- محكمة التمييز القطريّة الطعن رقم 49 لسنة 1986 ق- جلسة 1986/3/20.
- محكمة التمييز القطريّة الطعن رقم 44 لسنة 2008 – جلسة تاريخ 27-5-2008
- محكمة التمييز القطريّة- الأحكام الجنائيّة، الطعن رقم 18 لسنة 2009 ق، بتاريخ 2-2-2009.
- محكمة التمييز القطريّة- الأحكام الجنائيّة، الطعن رقم 152 لسنة 2009 ق، بتاريخ 15-6-2009.
- إدارة الفتاوى والعقود في قطر، (ف.ع 3/-11 1535/ 2003).

الأحكام المصرية:

- حكم المحكمة الإداريّة العليا الصادر في الطعن رقم 775 لسنة 13ق، جلسة 22\2\1969.
- محكمة النقض المصريّة – جنائيّ- الطعن رقم 23634 لسنة 67 ق- جلسة 2-6-1998.
- المحكمة الإداريّة العليا الطعن رقم 634 لسنة 3ق – تاريخ الجلسة 8-3-1985.
- المحكمة الإداريّة العليا الطعن رقم 1655 لسنة 2ق – جلسة تاريخ 14-12-1957.
- المحكمة الإداريّة العليا المصريّة، الطعن رقم 2998 لسنة 42 جلسة 8-8-1999.
- قرار محكمة القضاء التأديبي المصريّة، جلسة 12 يناير 1978، دعوى 905.
- المحكمة الإداريّة العليا، الطعن رقم 7688 لسنة 46 ق، جلسة 30-3-2002.
- المحكمة الإداريّة العليا الطعن رقم 2495 لسنة 30 قضائيّة- بتاريخ 17-06-1986.

التشريعات:

التشريعات القطريّة:

- قانون الإجراءات الجنائيّة القطريّ رقم (23) لسنة 2004.
- قانون الخدمة العسكرية رقم (31) لسنة 2006.
- قانون الموارد البشرية القطريّ رقم (15) لسنة (2016).

تشريعات أخرى:

- قانون رقم 150 لسنة 1950 بشأن قانون الإجراءات الجنائيّة، مصر.

نهاية البحوث والدراسات باللغة العربية

Appendix 1

Interview Questions

1. What are the main drivers for organisations in Qatar to adopt cloud computing?
2. How do organisations address vulnerabilities concerning data confidentiality in the cloud?
3. How can organisations ensure they retain data ownership when stored in the cloud?
4. What are the key differences between private and public cloud infrastructures?
5. Are there scenarios under existing laws where third parties can access data in the public cloud?
6. How significant is data sovereignty for Qatar from a national perspective?
7. Is Qatar using private clouds for sensitive information, and what are the challenges in developing such infrastructure?
8. What lessons have been learned since cloud service providers began operating in Qatar?
9. How do entities decide to migrate to the cloud, and is it optional?
10. What are the essential steps required before transitioning to the cloud?
11. What types of encryption are used for data stored in the cloud, and can cloud service providers access this data?
12. Are there data classifications that should not be moved to the cloud, and what are the storage strategies for such data?
13. What impacts are anticipated on the cloud computing landscape with new cloud service providers in Qatar?
14. What legal frameworks govern the cloud environment in Qatar, and which body oversees these services?
15. Did cloud service providers comply with specific local laws or regulations upon entering Qatar?
16. How does the USA PATRIOT Act affect Qatar's data sovereignty?
17. Are there ongoing academic research projects focusing on data sovereignty or cloud computing in Qatar?
18. What are the differences between data localisation and data sovereignty?
19. What improvements and regulatory changes are needed in Qatar's cloud computing scenario?
20. Could you share your background and experience in cloud computing?
21. Do you consent to mentioning your name, title, and organisation in this publication?

List of Abbreviations

Abbreviation	Full Form
IRB	Institutional Review Board
HBKU	Hamad Bin Khalifa University
QFZ	Qatar Free Zone
QNV2030	Qatar National Vision 2030
SDG	Sustainable Development Goals
TASMU	Qatar Smart Program
Qnbn	Qatar National Broadband Network
EM	Consumer Engagement Towards Energy Saving Behaviour
ML	Machine Learning
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
M-learning	Mobile Learning
CIA	Confidentiality, Integrity, and Availability
NIA	National Information Assurance
MCIT	Ministry of Communication and Information Technology
GCP	Google Cloud Platform
IoMT	Internet of Medical Things
IDS	Intrusion Detection System
DL	Deep Learning
DNN	Deep Neural Network
SVM	Support Vector Machine
KNN	K-Nearest Neighbours
BYOK	Bring Your Own Key
CRA	Communications Regulatory Authority
GDPR	General Data Protection Regulation
AI	Artificial Intelligence
MENA	Middle East and North Africa
NCSA	National Cybersecurity Agency - Qatar

- Yu, S., C. Wang, K. Ren, and W. Lou. "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing." In 2010 Proceedings IEEE INFOCOM, 1-9. IEEE, March 2010.
- Zainudeen, A., and D. Ratnadiwakara. "Digital Economies and Data Sovereignty in the MENA Region." ICT Policy Review, 2021.
- Zhang, Q., L. Cheng, and R. Boutaba. "Cloud Computing: State-of-the-Art and Research Challenges." Journal of Internet Services and Applications 1 (2010): 7-18.
- Zhang, X., and H. Chen. "Regulatory Frameworks for Data Sovereignty and Cloud Computing: A Comparative Analysis." Journal of Information Technology & Politics 17, no. 3 (2020): 215-231.
- Zhu, X., H. Liu, and S. Wei. "Cloud Computing Adoption in the Public Sector: A Meta-Analysis of Antecedents and Outcomes." Information Systems Frontiers 23, no. 5 (2021): 1229-1248.
- Zissis, D., and D. Lekkas. "Addressing Cloud Computing Security Issues." Future Generation Computer Systems 28, no. 3 (2012): 583-592.
- Zubair, M., D. Unal, A. Al-Ali, T. Reimann, and G. Alinier. "Cybersecurity for Next-Generation Healthcare in Qatar." Journal of Emergency Medicine, Trauma & Acute Care, Qatar Health 2020 Conference 2021, no. 2 (2021): 41.

- Turner, V., J. Kaplan, S. Thomas, and B. Saunders. "Software as a Service (SaaS): A Market and Financial Model." Future Generation Computer Systems 21, no. 3 (2003): 513-522.
- Vial, G. "Understanding Digital Transformation: A Review and a Research Agenda." The Journal of Strategic Information Systems 28, no. 2 (2019): 118-144.
- Wallen, J. "Disaster Recovery: IT's Most Important Task." TechRepublic. https://www.techrepublic.com/article/disaster-recovery-its-most-important-task/, 2018.
- Wang, C., Q. Wang, K. Ren, and W. Lou. "Ensuring Data Storage Security in Cloud Computing." In 2009 17th International Workshop on Quality of Service, 1-9. IEEE, July 2009.
- Wang, Q., C. Wang, K. Ren, W. Lou, and J. Li. "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing." IEEE Transactions on Parallel and Distributed Systems 22, no. 5 (2010): 847-859.
- Weber, A. S. "Can Cloud Computing Overcome Barriers to Education in the Middle East and North Africa (MENA) Region?" In Conference Proceedings of eLearning and Software for Education (eLSE), vol. 7, no. 01, 565-570. Carol I National Defence University Publishing House, 2011.
- Weerakkody, V., M. Janssen, and Y. K. Dwivedi. "Transformational Change and Business Process Reengineering (BPR): Lessons from the British and Dutch Public Sector." Government Information Quarterly 28, no. 1 (2016): 27-36.
- Wei, L., H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos. "Security and Privacy for Storage and Computation in Cloud Computing." Information Sciences 258 (2014): 371-386.
- Westerman, G., D. Bonnet, and A. McAfee. Leading Digital: Turning Technology into Business Transformation. Harvard Business Review Press, 2014.
- World Bank. Qatar GDP per Capita. World Bank Data, 2023.
- Yamin, M., and R. Ibrahim. "The Role of Leadership in Digital Transformation: A Review." Digital Transformation Review 8, no. 1 (2022): 30-45.
- Yan, Z., X. Li, M. Wang, and A. V. Vasilakos. "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing." IEEE Transactions on Cloud Computing 5, no. 3 (2015): 485-498.
- Yang, H., and M. Tate. "A Descriptive Literature Review and Classification of Cloud Computing Research." Communications of the Association for Information Systems 31, no. 1 (2012): 2-57.

- Rouse, M. "Infrastructure as a Service (IaaS)." TechTarget. https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS, 2019.
- Scarfone, K., and P. Mell. "Guide to Intrusion Detection and Prevention Systems (IDPS)." National Institute of Standards and Technology, 2007.
- Shapiro, C., and H. R. Varian. Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press, 1999.
- Sharim, L. "Challenges of Data Sovereignty in Cloud Computing: A Systematic Review." Journal of Cloud Computing 20, no. 2 (2021): 89-102.
- Shatilov, K., V. Boiko, S. Krendelev, D. Anisutina, and A. Sumaneev. "Solution for Secure Private Data Storage in a Cloud." In 2014 Federated Conference on Computer Science and Information Systems, 885-889. IEEE, September 2014.
- Singi, K., S. G. Choudhury, V. Kaulgud, R. J. C. Bose, S. Podder, and A. P. Burden. "Data Sovereignty Governance Framework." In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, 303-306, June 2020.
- Sood, S. K. "A Combined Approach to Ensure Data Security in Cloud Computing." Journal of Network and Computer Applications 35, no. 6 (2012): 1831-1838.
- Soofi, A. A., M. I. Khan, and F. E. Amin. "A Review on Data Security in Cloud Computing." International Journal of Computer Applications 96, no. 2 (2017): 95-96.
- Sookhak, M., F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya. "Attribute-Based Data Access Control in Mobile Cloud Computing: Taxonomy and Open Issues." Future Generation Computer Systems 72 (2017): 273-287.
- Sultan, N. "Cloud Computing: A Democratising Force?" International Journal of Information Management 33, no. 5 (2013): 810-815.
- Sun, Y., J. Zhang, Y. Xiong, and G. Zhu. "Data Security and Privacy in Cloud Computing." International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.
- Surbiryala, J., and C. Rong. "Cloud Computing: History and Overview." In 2019 IEEE Cloud Summit, 1-7, August 2019.
- Tang, J., Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya. "Ensuring Security and Privacy Preservation for Cloud Data Services." ACM Computing Surveys (CSUR) 49, no. 1 (2016): 1-39.

- Najafi, B., M. Amra, and A. Najafi. "Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar." In Exploring Global FinTech Advancement and Applications, 158-211. IGI Global, 2024.
- Nam, T., and T. A. Pardo. "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions." In Proceedings of the 12th Annual International Conference on Digital Government Research, 282-291. 2011.
- Nurdiani, I., M. S. Börjesson, and L. Angelis. "A Systematic Mapping Study on the Combination of Agile Software Development and Leadership Styles." Journal of Systems and Software 161 (2020): 110459.
- Okoli, C. "A Guide to Conducting a Standalone Systematic Literature Review." Communications of the Association for Information Systems 37, no. 1 (2015): 879-910.
- Omran, R. "A Qualitative Analysis of Cloud Computing Adoption Challenges in the Arabian Gulf Region." PhD diss., Colorado Technical University, 2020.
- Pallis, G. "Cloud Computing: The New Frontier of Internet Computing." IEEE Internet Computing 14, no. 5 (2010): 70-73.
- Peterson, Z. N. J., M. Gondree, and R. Beverly. "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud." In Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11). 2011.
- Qatar Cybersecurity Strategy. National Cybersecurity Strategy. Ministry of Transport and Communications, Qatar, 2020.
- Qatar Financial Centre. Personal Data Privacy Protection Law No. 13 of 2016. Qatar Financial Centre, 2020.
- Qatar National Vision 2030. Planning and Statistics Authority. http://www.psa.gov.qa/en/qnv/Pages/default.aspx, 2018.
- Qatar National Vision 2030. QNV 2030 Implementation Plan. Ministry of Planning and Statistics, Qatar, 2020.
- Q-CERT. Qatar Computer Emergency Response Team Annual Report. Q-CERT, 2021.
- Rehman, M. S., and M. F. Sakr. "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar." In 2011 IEEE Global Engineering Education Conference (EDUCON), 875-879. IEEE, 2011.

- Kuner, C., F. H. Cate, C. Millard, and D. J. B. Svantesson. "Data Protection and Privacy Laws in a Nutshell." Journal of Data Protection & Privacy 2, no. 1 (2017): 47-61.
- Kuner, C. "An International Legal Framework for Data Protection: Issues and Prospects." Computer Law & Security Review 25, no. 4 (2009): 307-317.
- Li, R., Z. Xu, W. Kang, K. C. Yow, and C. Z. Xu. "Efficient Multi-Keyword Ranked Query over Encrypted Data in Cloud Computing." Future Generation Computer Systems 30 (2014): 179-190.
- Li, Y., K. Gai, L. Qiu, M. Qiu, and H. Zhao. "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing." Information Sciences 387 (2017): 103-115.
- Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi. "Cloud Computing—The Business Perspective." Decision Support Systems 51, no. 1 (2011): 176-189.
- Martin, S., R. Moore, and J. Redshaw. "Public Sector Leadership in the Digital Age: Navigating through Disruption." Public Administration Review 79, no. 5 (2019): 687-693.
- Medawar, S. "Information Retrieval in Systematic Reviews: Challenges and Opportunities." Information Processing & Management 58, no. 1 (2021): 102389.
- Mell, P., and T. Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology 53, no. 6 (2011): 50-51.
- Menezes, A. J., P. C. Van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
- Middleton, A. M. "Data-Intensive Technologies for Cloud Computing." In Handbook of Cloud Computing, 83-136. 2010.
- Milford, T., and B. George. "Data Sovereignty and the Cloud: A Board and Executive Officer's Guide." Journal of Cloud Computing: Advances, Systems and Applications 8, no. 1 (2020): 1-12.
- Ministry of Transport and Communications. Qatar Smart Program (TASMU). Ministry of Transport and Communications, 2019.
- Mishra, M., I. Arora, P. Singh, and S. Prabhakar. "An Assessment of Cloud Computing: Evolution." Journal of Cloud Computing: Advances, Systems and Applications, 2020.

- Irion, K. "Government Cloud Computing and National Data Sovereignty." Policy & Internet 4, no. 3-4 (2012): 40-71.
- Istepanian, R. S. H., S. Hu, N. Y. Philip, and A. Sungoor. "The Potential of Internet of Medical Things (IoMT) for Healthcare Applications." Journal of Healthcare Engineering 2, no. 3 (2011): 309-318.
- Janssen, M., E. Estevez, and T. Janowski. "Interoperability in Big, Open, and Linked Data–Organizational Maturity, Capabilities, and Data Portfolios." Government Information Quarterly 31, no. 3 (2014): S57-S68.
- Johansson, J., L. Sundberg, and S. Mattsson. "Leadership Styles and Their Influence on Digital Transformation in Public Sector Organizations." Journal of Public Administration Research and Theory 31, no. 1 (2021): 125-139.
- Jordan, M. I., and T. M. Mitchell. "Machine Learning: Trends, Perspectives, and Prospects." Science 349, no. 6245 (2015): 255-260.
- Kallio, H., A.-M. Pietilä, M. Johnson, and M. Kangasniemi. "Systematic Methodological Review: Developing a Framework for a Qualitative Semi-Structured Interview Guide." Journal of Advanced Nursing 72, no. 12 (2016): 2954-2965.
- Kaplan, J., T. Bailey, C. Rezek, and D. O'Halloran. "Cybersecurity: A Necessary Foundation for the Future." McKinsey & Company, 2016. https://www.mckinsey.com/business-functions/risk/our-insights/cybersecurity-a-necessary-foundation-for-the-future.
- Kasiwi, A., M. Ikeda, and D. Anderson. "Rethinking Data Sovereignty in Cloud Computing." Journal of Data Sovereignty 15, no. 1 (2022): 142-155.
- Kaufman, L. M. "Data Security in the World of Cloud Computing." IEEE Security & Privacy 7, no. 4 (2009): 61-64.
- King, N. J., and V. T. Raja. "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud." Computer Law & Security Review 28, no. 3 (2012): 308-319.
- KPMG. "Doing Business in Qatar: Investment Opportunities and Challenges." KPMG, 2021.
- Kronabeter, A., and S. Fenz. "Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation." In Cloud Computing: Third International Conference, CloudComp 2012, Vienna, Austria, September 24-26, 2012, Revised Selected Papers 3, 114-123. Springer International Publishing, 2013.

- Giese, T., and R. Anderl. "Maintaining Control over Distributed Data through a Data Sovereignty Model." In 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), 1-7, November 2022.
- Gil-Garcia, J. R., N. Helbig, and A. Ojo. "Being Smart: Emerging Technologies and Innovation in the Public Sector." Government Information Quarterly 31, no. S1 (2014): S2-S8.
- Gong, Y., X. Hu, and H. Liu. "Leadership Styles, Team Dynamics, and Information Technology Service Innovation: Evidence from the Chinese Public Sector." Journal of Public Administration Research and Theory 30, no. 1 (2020): 47-66.
- Hairi, N. A. "World Reaction and the Role of Turkiye, Iran, and Asian Countries in Maintaining Qatar Sovereignty: A Case Study of Gulf Crisis." Sains Insani 8, no. 2 (2023): 168-173.
- Harris, J., L. Croot, J. Thompson, and J. Springett. "How Stakeholder Participation Can Contribute to Systematic Reviews of Complex Interventions." Journal of Epidemiology and Community Health 70, no. 2 (2014): 207-214.
- Hashem, I. A. T., I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan. "The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues." Information Systems 47 (2015): 98-115.
- Hashizume, K., D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez. "An Analysis of Security Issues for Cloud Computing." Journal of Internet Services and Applications 4, no. 1 (2013): 1-13.
- Heeks, R., and C. Stanforth. "Technological Change in Developing Countries: Opening the Black Box of Process Using Actor-Network Theory." Development Studies Research 2, no. 1 (2015): 33-50.
- Hellmeier, M., J. Pampus, H. Qarawlus, and F. Howar. "Implementing Data Sovereignty: Requirements and Challenges from Practice." In Proceedings of the 18th International Conference on Availability, Reliability and Security, 1-9, August 2023.
- Houghton, J. D., A. Carnes, and C. N. Ellison. "A Cross-Sectional Examination of Transformational Leadership and Transformational Leaders in the United States." Leadership Quarterly 26, no. 3 (2015): 437-447.
- Huang, Z., and M. Benyoucef. "From E-Commerce to Social Commerce: A Close Look at Design Features." Electronic Commerce Research and Applications 12, no. 4 (2015): 246-259.

- Clohessy, T., T. Acton, and L. Morgan. "Smart City as a Service (SCaaS): A Future Roadmap for E-Government Smart City Cloud Computing Initiatives." Digital Policy, Regulation and Governance 19, no. 1 (2017): 58-69.
- Connett, W., and T. Johnson. "Updating Systematic Reviews: An International Survey." PLoS ONE 8, no. 7 (2013): e67145. https://doi.org/10.1371/journal.pone.0067145.
- Cordella, A., and N. Tempini. "E-Government and Organizational Change: Reappraising the Role of ICT and Bureaucracy in Public Service Delivery." Government Information Quarterly 32, no. 3 (2015): 279-286.
- Cortellazzo, L., E. Bruni, and R. Zampieri. "The Role of Leadership in a Digitalized World: A Review." Frontiers in Psychology 10 (2019): 1938. https://doi.org/10.3389/fpsyg.2019.01938.
- Creswell, J. W., and J. D. Creswell. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 5th ed. SAGE Publications, 2017.
- Creswell, J. W., and C. N. Poth. Qualitative Inquiry and Research Design: Choosing among Five Approaches. 4th ed. SAGE Publications, 2017.
- De Hert, P., and V. Papakonstantinou. "Three Scenarios for International Data Privacy Governance: Towards a Global Data Privacy Organization, Preferably a UN Agency." ISJLP 9 (2013): 271-300.
- Eaton, C. "Platform as a Service (PaaS)." Gartner IT Glossary, 2010. https://www.gartner.com/en/information-technology/glossary/platform-as-a-service-paas.
- Elidrisy, A. "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar." Journal of Innovative Research 2, no. 1 (2024): 20-28.
- Esposito, C., A. Castiglione, and K. K. R. Choo. "Encryption-Based Solution for Data Sovereignty in Federated Clouds." IEEE Cloud Computing 3, no. 1 (2016): 12-17.
- Finlay, L. "Negotiating the Swamp: The Opportunity and Challenge of Reflexivity in Research Practice." Qualitative Research 2, no. 2 (2002): 209-230.
- Garrison, G., R. L. Wakefield, and S. Kim. "The Effects of IT Capabilities and Delivery Model on Cloud Computing Success and Firm Performance for Cloud-Supported Processes and Operations." International Journal of Information Management 35, no. 4 (2015): 377-393.
- GCC-STAT. GCC Statistical Centre: Data Sovereignty and Cloud Computing. GCC-STAT, 2022.

- Banse, C. "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" In Proceedings of the 2021 on Cloud Computing Security Workshop, 153-154, November 2021.
- Bass, B. M., and R. E. Riggio. Transformational Leadership. Mahwah, NJ: Lawrence Erlbaum Associates, 2006.
- Bertot, J. C., P. T. Jaeger, and J. M. Grimes. "Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies." Government Information Quarterly 27, no. 3 (2010): 264-271.
- Biočić, B., D. Tomić, and D. Ogrizović. "Economics of Cloud Computing." In 2011 Proceedings of the 34th International Convention MIPRO, 1438-1442. IEEE, May 2011.
- Braun, V., and V. Clarke. "Using Thematic Analysis in Psychology." Qualitative Research in Psychology 3, no. 2 (2006): 77-101. https://doi.org/10.1191/1478088706qp063oa.
- ———. "Thematic Analysis." In APA Handbook of Research Methods in Psychology, Vol. 2: Research Designs, edited by H. Cooper, 57-71. APA, 2012.
- Buyya, R., J. Broberg, and A. Goscinski, eds. Cloud Computing: Principles and Paradigms. Wiley, 2018.
- Calzada, I. Data Sovereignty in the Age of Big Tech: Political Geographies of Data and Challenges of Decentralized Alternatives. Oxford University Press, 2021.
- Castleberry, A., and A. Nolen. "Thematic Analysis of Qualitative Research Data: Is It as Easy as It Sounds?" Currents in Pharmacy Teaching and Learning 10, no. 6 (2018): 807-815. https://doi.org/10.1016/j.cptl.2018.03.019.
- Celeste, E. "Data Sovereignty and the Cloud: A Board Game with Many Players." Computer Law & Security Review 40 (2021): 105486. https://doi.org/10.1016/j.clsr.2020.105486.
- Chakraborty, S., and K. Joseph. ICT and Digital Transformation in the Middle East. Routledge, 2021.
- Chandrasekaran, A., and M. Kapoor. "State of the Public Cloud: The Cloud Adoption Conundrum." Infosys Labs Briefings 9, no. 1 (2011): 3-10.
- Chatterjee, S., N. P. Rana, and Y. K. Dwivedi. "Examining the Role of Transformational Leadership in Cloud Security Management: A Quantitative Study." Information Technology & People 32, no. 6 (2019): 1325-1351.
- Choo, K. K. R. "Legal Issues in the Cloud." IEEE Cloud Computing 1, no. 01 (2014): 94-96.

- Almorsy, M., J. Grundy, and I. Müller. "An Analysis of the Cloud Computing Security Problem." Communications of the ACM 59, no. 1 (2016): 38-46.
- Al-Naama, M. "Data Sovereignty in the GCC: Legal and Regulatory Perspectives." Gulf Affairs, 2022.
- Alnaemi, S. R. "The Gulf Crisis and Rise of Digital Nationalism in Qatar: A Case Study of Tweets." Master's thesis, 2021.
- Al-Qahtani, F., and E. A. Abu-Shanab. "End User Satisfaction with Cloud Computing: The Case of Hamad Medical Corporation in Qatar." International Journal of Healthcare Information Systems and Informatics 16, no. 4 (2021): 1-23. https://doi.org/10.4018/IJHISI.2021100101.
- Alsalemi, A., A. Al-Kababji, Y. Himeur, F. Bensaali, and A. Amira. "Cloud Energy Micro-Moment Data Classification: A Platform Study." In 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC), 420-425. IEEE, 2020.
- Alshamaila, Y., S. Papagiannidis, and F. Li. "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework." Journal of Enterprise Information Management 26, no. 3 (2013): 250-275. https://doi.org/10.1108/JEIM-09-2012-0054.
- Al-Sharim, H. A. "The Privacy in the Cloud: An Examination of the Law in Qatar." PhD diss., Hamad Bin Khalifa University, 2021.
- Alshomrani, S., and S. Qamar. "Cloud-Based E-Government: Benefits and Challenges." International Journal of Multidisciplinary Sciences and Engineering 4, no. 6 (2013): 1-9.
- Alzadjali, K., and A. Elbanna. "Smart Institutional Intervention in Adopting Digital Infrastructure: The Case of Government Cloud Computing in Oman." Information Systems Frontiers 22, no. 2 (2020): 365-380. https://doi.org/10.1007/s10796-019-09915-7.
- Baker McKenzie. "Qatar: Data Protection Overview." Baker McKenzie, 2021.
- Banerjee, P. "Governing the Cloud: Policy Strategies for Data Sovereignty and Digital Infrastructure." Digital Policy, Regulation and Governance 24, no. 2 (2022): 125-137.
- Bannister, F., and R. Connolly. "ICT, Public Values and Transformative Government: A Framework and Programme for Research." Government Information Quarterly 31, no. 1 (2014): 119-128.

sovereignty, regulatory compliance, and cloud security. The paper highlights the significance of geographical localization for maintaining data sovereignty and examines the impact of international laws such as the USA PATRIOT Act and the CLOUD Act. It contrasts public and private cloud infrastructures, emphasizing the trade-offs between control, security, cost, and scalability. The study also underscores the importance of disaster recovery, business continuity, and effective collaboration between cloud providers and clients. The paper's findings challenge existing models and theories, providing new perspectives on the interaction between local and international legal frameworks. It offers practical recommendations for policymakers, cloud service providers, and businesses, emphasizing tailored strategies, robust cybersecurity measures, and best practices in data management. Future research directions include exploring emerging technologies and evolving legal landscapes in cloud computing. Overall, this paper contributes valuable insights to the academic field, offers practical guidance for stakeholders, and lays the groundwork for further research in cloud data sovereignty. The findings are relevant not only to Qatar but also to other nations facing similar challenges in cloud computing.

Bibliography

- Abulhussain, F. M. "A Study Evaluating the Readiness Level for Qatar Companies to Adopt Industry 4.0." Master's thesis, 2021.
- Abu-Taieh, E., A. Alfaries, S. Al-Otaibi, and G. Aldehim. "Cybersecurity Crime and Punishment: A Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia." International Journal of Cyber Warfare and Terrorism 8, no. 3 (2018): 46-59. https://doi.org/10.4018/IJCWT.2018070104.
- Ahmed, R., and J. Campbell. "The Role of Leadership and Governance in Transforming Public Sector Organizations: A Review and Future Research Agenda." Public Administration Quarterly 45, no. 3 (2021): 345-375.
- Albrecht, J. P. "How the General Data Protection Regulation Will Change Our World." Journal of Privacy and Data Protection 2, no. 2 (2016): 84-90.
- Aldossary, S., and A. Saad. "Cloud Computing Approaches, Characteristics and Cloud Computing Status in the Arab World." Multi-Knowledge Electronic Comprehensive Journal for Education & Science Publications, no. 25 (2019): 1-18.
- Ali, H. B. Y., L. M. Abdullah, M. Kartiwi, A. Nordin, N. Salleh, and N. S. A. A. Bakar. "A Systematic Literature Mapping of Extensive Data Risk Analysis in a Cloud Computing Environment." In Journal of Physics: Conference Series, vol. 1018, no. 1, p. 012017. IOP Publishing, 2018.

frameworks and urging cloud providers to comply with local laws. This paper recommends data accessibility rules to protect national security and privacy, ensuring cloud data meets standards. It suggests bilateral agreements with cloud server countries to give Qatar legal authority over foreign data and urges cloud providers to invest in security while adhering to Qatari laws. The paper advises creating Qatar-specific cloud options for greater control and emphasizes the importance of regular audits to ensure compliance with evolving data security laws. It also calls for more research on international cloud data sovereignty regulations, especially for small countries like Qatar, highlighting the challenges of balancing innovation with strict data management.

5.3. Theoretical Implications

To strengthen the discussion of theoretical and practical implications, this study's findings can be linked explicitly to leadership and data sovereignty theories. Theoretically, this research contributes to transformational leadership theory by demonstrating how leadership styles significantly influence the successful adoption of cloud computing in the public sector. It highlights how leaders with strategic foresight, risk management skills, and collaborative approaches can drive digital transformation, particularly in complex environments like Qatar. Additionally, the study extends data sovereignty theory by exploring how local legal frameworks interact with global cloud computing standards, offering new insights into the balance between national security concerns and international data-sharing requirements.

For practical implications, the study provides actionable recommendations for policymakers and public sector leaders. Specifically, it suggests the need for leadership training focused on managing ICT integration and cloud computing adoption. Additionally, it recommends that policymakers develop clear guidelines on data sovereignty and compliance with international regulations to ensure secure cloud usage. Public sector organizations should also focus on fostering partnerships with global cloud service providers while maintaining compliance with national legal frameworks. By addressing these recommendations, practitioners can better navigate the complex landscape of cloud adoption, data security, and regulatory compliance in the digital age.

6. Conclusion

This paper comprehensively explores cloud data sovereignty in Qatar, offering insights into the complexities of cloud computing within a national context. By integrating literature reviews and interviews, it reveals key themes like data

data protection challenges. A key finding emphasizes the importance of aligning cloud strategies with national and international laws, as compliance is vital for data security. Interviewees, including Elidrisy[95] and Interviewee 4, stress the need to understand extraterritorial laws like the USA PATRIOT Act and CLOUD Act, which may threaten data sovereignty. Balancing cloud security with user privacy is another critical issue, with scholars like Alsalemi et al.[96] and Zubair et al.[97] noting the complexities of implementing robust encryption while safeguarding privacy. The choice between public and private cloud systems also impacts data security, particularly in Qatar's context, where privacy and control are paramount. Finally, the issue of vendor lock-in raises concerns for Qatari businesses, highlighting the need for strategies that ensure flexibility and competitive cloud service options. Understanding these dynamics is essential for Qatar's cloud computing strategies, which aim to foster economic growth and innovation while maintaining security and privacy.

5. Discussion and Recommendations

5.1. Discussion

This section addresses cloud environment issues in Qatar and globally, focusing on key findings and their relevance to cloud data security. It explores Qatar's complex data privacy policy, shaped by evolving legislation, technologies, and political factors, and highlights the challenges of balancing local and international laws, such as the USA PATRIOT Act and CLOUD Act. Public clouds offer cost savings but raise security concerns, while private clouds align with Qatar's sovereignty standards, offering greater control. Qatar's approach to cloud data management, emphasizing flexibility and multiple providers, mirrors global trends, underscoring the need for ongoing research in this evolving field.

5.2. Recommendations

This paper enhances cloud computing and data security theories, focusing on Qatar's unique context. It highlights the complex interplay between technology, law, and geopolitics, revealing gaps in existing models. The study integrates international laws, like the CLOUD Act, with local regulations, recommending adaptable legal

(95) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," Journal of Innovative Research 2, no. 1 (2024): 20–28.

(96) A. Alsalemi et al., "Cloud Energy Micro-Moment Data Classification: A Platform Study," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC) (2020): 420–425.

(97) M. Zubair et al., "Cybersecurity for Next-Generation Healthcare in Qatar," Journal of Emergency Medicine, Trauma & Acute Care, Qatar Health 2020 Conference 2021, no. 2 (2021): 41.

4.3. Integration of Interview and Literature Review Findings

The paper's literature review and interviews offer diverse perspectives on Qatari data sovereignty and cloud computing, highlighting key areas of agreement and divergence. The focus on data control and legal compliance reflects significant progress. Both Elidrisy[91] and Al-Sharim[92] align with interviewees on stringent data governance practices, emphasizing the importance of adhering to local and international laws. Concerns about compliance with foreign legislation like the USA PATRIOT Act and the CLOUD Act underscore the complexities of data sovereignty in a global context. Security perceptions varied, with Alsalemi et al.[93] providing a strong data classification framework, though interviewees expressed differing levels of trust in cloud security. This suggests a disconnection between academic research and real-world cloud security concerns. There is growing consensus on the benefits of private cloud systems, with Najafi et al.[94] and interviewees agreeing on enhanced security and control. However, vendor lock-in concerns, raised in interviews, are underexplored in literature, indicating a research gap. Interviewees provided deeper insights into disaster management and cloud operations, suggesting the need for more targeted research. The interviews contribute valuable, unique data, enhancing the understanding of cloud computing challenges in Qatar. Qatar's cloud computing landscape ties data sovereignty to advanced technologies. Robust encryption, like Attribute-Based Encryption (ABE), offers refined access control but faces practical challenges due to its complexity. Homomorphic encryption enhances privacy, especially in sensitive sectors, but its computational demands are a hurdle. Data localization aligns with national laws but may limit global interoperability. Balancing these technologies with practical cloud realities is crucial for Qatar's digital ambitions.

4.4. Discussion of Key Findings

Al-Thani et al. (2020) explore the intricate interplay between Qatar's rapid technological advancements in cloud computing and its evolving social norms and group demands. Their study highlights the delicate balance between embracing cloud technology and preserving societal values, crucial in addressing Qatar's cloud

(91) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," Journal of Innovative Research 2, no. 1 (2024): 20–28.

(92) H. A. Al-Sharim, "The Privacy in the Cloud: An Examination of the Law in Qatar" (PhD diss., Hamad Bin Khalifa University, 2021).

(93) A. Alsalemi et al., "Cloud Energy Micro-Moment Data Classification: A Platform Study," in 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC) (2020): 420–425.

(94) B. Najafi, M. Amra, and A. Najafi, "Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar," in Exploring Global FinTech Advancement and Applications (IGI Global, 2024): 158–211.

4.2.3. Cloud Security and Privacy Concerns

Cybersecurity issues, including data protection and encryption, were discussed. The goal was to strike a balance between security and cloud vulnerability. "Cloud computing has many benefits but complex security issues," said a scholar. Increased encryption and monitoring are needed to prevent data leaks. This comment shows how hard it is to manage cloud security with evolving threats. Participants explored the delicate privacy-accessibility balance. A privacy expert said, "Encryption and strict access controls are necessary, but they shouldn't get in the way of the user experience or make cloud services less useful." Users and providers struggle to balance security and usability in the cloud.

4.2.4. Vendor Lock-in and Flexibility in Cloud Services

According to interviews, Qatar's cloud service alternatives and flexibility are hampered by vendor lock-in. Managing hazards and having various cloud providers were discussed. Expert said: "It's hard to avoid vendor lock-in." Comparing services and ensuring compatibility is necessary for cloud migration. You must carefully select providers so you can switch, and no seller has too much power or authority. An expert noted as well, "Having multiple cloud providers in Qatar prevents vendor lock-in and encourages competition, which leads to better services and new ideas." This principle suggests multiple providers create a healthy, competitive market that rewards customers with better service and new ideas. Interviews revealed that cost is the primary barrier to cloud adoption in Qatar. Participants discussed cost reduction, scalability, and resource management, emphasizing that the potential savings and efficient resource use drive cloud service adoption. An academic noted, "Scalability is a key economic factor," allowing businesses to adjust resources without heavy infrastructure investment. However, concerns about provider lock-in and economic factors impact strategic cloud decisions. Qatar's decision-makers must balance efficiency, scalability, cost, and vendor relationships to ensure successful cloud computing implementation, reflecting the nuanced challenges of cloud utilization in the region. Interviews also highlighted the importance of disaster recovery and business continuity in Qatari cloud operations. Companies moving to the cloud are concerned about data security and redundancy. One expert emphasized, "Strong disaster recovery solutions drove our cloud adoption." Cloud services enable business continuity during crises, with redundancy ensuring smooth operations. This underscores the need for comprehensive disaster recovery plans beyond data backup. The interviews stressed the importance of collaboration and communication with cloud providers. Experts noted that strong provider relationships enhance service delivery, problem-solving, and goal alignment, which are crucial for successful cloud adoption in Qatar.

4.2. Analysis of Interviews

For this paper, experts, policymakers, and researchers discussed cloud computing and data sovereignty in Qatar. Interviews were aimed at eliciting deep, deliberate responses, and recordings were examined for central themes. Significant priorities include Data Sovereignty, Geographic Localization, Regulatory Compliance, and Legal Framework.

4.2.1. Data Sovereignty and Geographical Localization

Data sovereignty and regional localization highlight the challenges of data governance in specific regions. Participants emphasized the importance of storing data within Qatar or under an EU regional agreement, ensuring compliance with local laws. Geographic localization is crucial for data security and aligning with legal requirements, especially where national laws strictly govern privacy and security. "Keeping data within national borders is essential for sovereignty," an interviewee noted. This underscores the legal and regulatory power over data location. Geographical localization offers control but faces limitations in a global digital environment where data crosses borders, complicating efforts to maintain control over cloud software. The interviews revealed the complexities of cloud computing laws, particularly how Qatar's evolving policies intersect with foreign legislation like the USA PATRIOT Act and CLOUD Act. Balancing local and international laws is critical for Qatar's secure data management amid its digital transformation.

4.2.2. Public vs. Private Cloud Considerations

This theme examines the impact of private versus public cloud infrastructures on Qatari data ownership, security, and control. People indicated that cloud options meet different data security and ownership concerns. "Private clouds offer greater control and security, which fits well with the needs of sensitive government data," said a tech. They cost more and grow slower than public clouds. Private clouds give more control and safety but may be less scalable and cost-effective than public clouds. However, public clouds, hosted by outside companies, are flexible and cheap but create privacy and security concerns. "Public clouds are shared environments where data is stored off-premises," a government expert stated. "This brings up questions about jurisdictional control and access." This raises concerns that public cloud data may be subject to the cloud provider's country laws. The theme compares public and private clouds under Qatar's unique security and regulation framework. It suggests we need a balanced, possibly hybrid, approach to optimise sovereignty and operational efficiency.

of data effectively. This aspect is particularly pertinent for economies like Qatar, which are in the process of diversifying and digitalizing. The robust computational capabilities offered by cloud computing can significantly bolster Qatar's initiatives in sectors such as healthcare, education, and smart city development, aligning with the country's National Vision 2030. Giese and Anderl[87] highlight the challenge of controlling distributed data in global collaborations, a key concern for Qatar's international partnerships in technology and education. Ensuring data sovereignty is crucial for protecting Qatar's economic development and sustainability.

The Interplay between Cloud Computing, Data Sovereignty, and Regulatory Compliance

The equilibrium between cloud computing, data sovereignty, and regulatory compliance is critical for countries like Qatar. Blancato (2023, 251) investigates the European Union's strategy in managing cloud data migration and reducing reliance on non-EU cloud service providers. This analysis is relevant to Qatar, offering insights into how a region can maintain data sovereignty while leveraging global cloud computing services. The study implies that for Qatar, aligning cloud strategies with national interests and security concerns is as vital as ensuring technical efficiency. Banse[88] addresses the intricate concept of data sovereignty in the cloud, unravelling the technical and regulatory complexities entwined in this sphere. This research is particularly pertinent to Qatar, as it navigates its cloud computing strategy amidst an evolving international legal landscape.

Technological Innovations and Challenges in Ensuring Data Sovereignty in the Cloud

Technological innovations and challenges play a significant role in ensuring data sovereignty in the cloud, a topic critical for Qatar's digital strategy. Yang et al.[89] focus on the key issues of data security and privacy protection within the cloud environment. This area is of paramount importance for Qatar as it advances its cloud computing capabilities. The study provides insights into various security measures and privacy protection strategies, essential for Qatar to maintain data integrity and sovereignty. Research[90] contribute to this discussion by examining big data processing techniques in cloud computing environments. Their research offers Qatar perspectives on managing the challenges associated with big data in the cloud. This is particularly relevant as Qatar continues to grow its digital infrastructure and services, generating and processing large volumes of data.

(87) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(88) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(89) H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research," Communications of the Association for Information Systems 31, no. 1 (2012): 2–57.

(90) C. Kuner, "An International Legal Framework for Data Protection: Issues and Prospects," Computer Law & Security Review 25, no. 4 (2009): 307–317.

Healthcare Sector's Adoption of Cloud Computing in Qatar:

Al-Qahtani and Abu-Shanab[85] research on cloud computing in Qatar's health business illustrates how it has revolutionised care. According to the report, cloud computing saves resources; thus, more healthcare organisations are using it. The study found that trust, compliance concerns, economic and operational benefits, and functional benefits most affect user happiness. The study also recommends fixing private cloud management and risk issues. Data sovereignty issues arise when healthcare uses the cloud, especially when protecting sensitive health data. Cloud technology in healthcare must be fast, safe, and compliant. A comprehensive examination of cloud healthcare demonstrates that cloud technology can enhance Qatari healthcare but potentially threaten data privacy and sovereignty.

Legal and Regulatory Challenges in Cloud Computing:

Qatar requires cloud computing regulations because they are new. Al-Sharim's 2021 assessment of Qatar's cloud privacy challenges found that cloud data standards are failing. The report dislikes Qatar's cloud computing and privacy laws. It demands more vital cloud data ownership and use rules. This topic impacts cloud software safety and international use. Qatar must amend its cloud computer legislation like many others. This adjustment is needed to maximise cloud computing without compromising data security and privacy. Data privacy and laws governing cloud data storage, processing, and sending are the focus of this theme. Qatar should implement Al-Sharim's advice to fix cloud computer issues immediately. There are privacy, data security, and international law rules. How law and technology interact is crucial to this issue. Qatar needs rigorous data protection standards for industry and society to adopt cloud computing. Qatar must demonstrate safe and honest cloud computing to create trust in cloud technology.

Cloud Computing's Role in Enhancing National Economies and Sustainable Development

The impact of cloud computing on national economies and sustainable development is profound and multifaceted. In their study, Hashem et al.[86] delve into the exponential growth of big data driven by cloud computing. They underscore the crucial need for substantial computational infrastructure to manage this burgeoning volume

(85) F. Al-Qahtani and E. A. Abu-Shanab, "End User Satisfaction with Cloud Computing: The Case of Hamad Medical Corporation in Qatar," International Journal of Healthcare Information Systems and Informatics 16, no. 4 (2021): 1–23

(86) I. A. T. Hashem et al., "The Rise of 'Big Data' on Cloud Computing: Review and Open Research Issues," Information Systems 47 (2015): 98–115.

Zone. The QFZ, a crucial project, shows how cloud technology and economic growth may work together by encouraging corporate growth and innovation. This initiative supports sustainable development goals such as Decent Work and Economic Growth (SDG 8), Industry, Innovation, and Infrastructure (SDG 9), and Sustainable Cities and Communities (SDG 11). Since it uses the cloud, this alignment represents a paradigm change toward an eco-friendlier and more sustainable city lifestyle, which aligns with SDG 13: Climate Action and other global environmental challenges.

Legal Frameworks and Privacy Concerns in Cloud Computing

Al-Sharim's 2021 analysis details Qatar's complex cloud computing rules, focusing on privacy and data security rules. The analysis reveals how difficult it is for Qatar to keep cloud data private because cloud services are utilised worldwide, and the USA PATRIOT Act applies to numerous countries. This issue is crucial to data sovereignty since international rules may trump local ones. People in other countries can access cloud data. Data sovereignty in Qatar requires robust, clear, and enforceable regulations to protect cloud data from unauthorized access and ensure compliance with international standards. While Qatar has made strides in developing its digital data laws, gaps remain, particularly regarding international legal challenges. These jurisdictional issues complicate Qatar's data sovereignty goals, potentially undermining national laws. The paper highlights Qatar's proactive adoption of cloud technology to support its national vision and environmental goals, while also addressing the legal complexities of data privacy and authority. This analysis underscores the intricate balance between technological advancement and legal challenges in achieving Qatar’s ambitions.

Impact of Cloud Computing on the Financial Sector and Data Security in Qatar:

Najafi et al.[84] found FinTech growing in Qatar. Cloud computing is crucial to changing the finance industry. Qatar's FinTech activities heavily rely on banking services, so this development is vital. Cloud computing simplifies and improves financial services, improving banking and payment services. It's not simple with this shift. The report raises concerns about financial transaction data laws and security hazards. With the government's financial and legal support, this fast growth illustrates that leveraging cloud technology for financial improvement is a plan.

(84) B. Najafi, M. Amra, and A. Najafi, “Exploring Global Fintech Advancement and Application: Case of Saudi Arabia, Turkey, and Qatar,” in Exploring Global FinTech Advancement and Applications (IGI Global, 2024): 158–211.

This paper selected 15 diverse pieces of literature to explore Qatari data sovereignty, addressing legal, scientific, and business challenges and opportunities[77]. The careful selection ensured a comprehensive analysis, focusing on Qatar's regulatory challenges and using Qatar-specific data for relevant insights into the nation's cloud infrastructure upgrades[78]. In this paper, a comprehensive examination of Qatar's legal landscape, technical challenges, and benefits of adopting a sovereign cloud model was conducted. The study focused on understanding Qatar's data sovereignty legislative frameworks, particularly the Qatar Financial Centre Data Security Regulations 2021 and the Qatar Personal Data Protection Law (PDPPL). Additionally, it assessed the technical aspects of implementing a sovereign cloud model in Qatar, analyzing technological limitations and advantages. This paper acknowledges its limitations, primarily the exclusive use of Google Scholar and Scopus, potentially limiting source diversity on data sovereignty in Qatar[79]. The focus on peer-reviewed articles from 2010-2023 may introduce publication bias[80], and the small selection of 15 studies could affect comprehensiveness[81]. The emphasis on Qatari issues may limit broader applicability[82]. Addressing these limitations would enhance the study's robustness and provide a more comprehensive analysis of data sovereignty in Qatar's evolving digital landscape.

4. Results and Findings

4.1. Findings from Existing Review

Integration of Cloud Computing with National Vision and Sustainability Initiatives

Elidrisy[83] noted that cloud computing in Qatar's national strategies and environmental programs supports QNV2030. This plan promotes a knowledge-based economy with cloud computing for Msheireb Downtown Doha and the Qatar Free

(77) A. Kasiwi, M. Ikeda, and D. Anderson, "Rethinking Data Sovereignty in Cloud Computing," Journal of Data Sovereignty 15, no. 1 (2022): 142–155.

(78) I. Calzada, Data Sovereignty in the Age of Big Tech: Political Geographies of Data and Challenges of Decentralized Alternatives (Oxford University Press, 2021).

(79) S. Medawar, "Information Retrieval in Systematic Reviews: Challenges and Opportunities," Information Processing & Management 58, no. 1 (2021): 102389.

(80) J. Harris et al., "How Stakeholder Participation Can Contribute to Systematic Reviews of Complex Interventions," Journal of Epidemiology and Community Health 70, no. 2 (2014): 207–214.

(81) A. Kasiwi, M. Ikeda, and D. Anderson, "Rethinking Data Sovereignty in Cloud Computing," Journal of Data Sovereignty 15, no. 1 (2022): 142–155.

(82) C. Okoli, "A Guide to Conducting a Standalone Systematic Literature Review," Communications of the Association for Information Systems 37, no. 1 (2015): 879–910.

(83) A. Elidrisy, "Leveraging Cloud Services & Digital Transformation for Sustainability: Insights from Cases of Qatar," Journal of Innovative Research 2, no. 1 (2024): 20–28.

Criteria Type	Criteria	Description
Inclusion	Peer-Reviewed Sources	Focus on peer-reviewed sources to ensure reliabili-.ty and accuracy
Inclusion	Relevant Case Studies and National Legislation	Case studies and relevant national legislation should be included for a comprehensive .examination
Inclusion	Publication Date Range ((2010-2023	It is limited to publications from 2010 to 2023 to .capture recent advancements
Exclusion	Non-Peer-Reviewed and Biased Sources	Exclusion of sources lacking peer review or .exhibiting potential bias
Exclusion	Irrelevant or Redundant Entries	Remove duplicates and entries unrelated to the .research questions

Table 6: Inclusion & Exclusion Criteria

The literature review began with 950 sources, narrowed to 341 after removing duplicates and irrelevant entries. After further screening, 129 papers required closer examination, with only 15 meeting the critical criteria for the systematic review. This meticulous selection process ensured the inclusion of high-quality, relevant studies focused on Qatar's cloud computing data privacy.

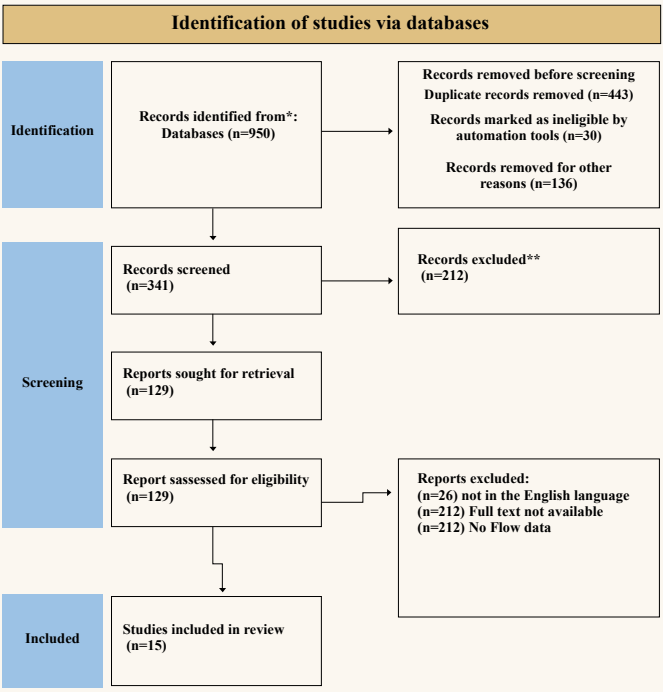


Figure 2: PRISMA Flow Chart

to provide a comprehensive and balanced understanding of the technological, regulatory, and governance challenges impacting data sovereignty in Qatar.

3.2.2. Data Collection

This paper involved semi-structured interviews with six experts in cloud computing, law, and data management in Qatar. Participants included two cloud professionals, two academic experts, one cloud service provider expert, and one security specialist. Ethical considerations ensured privacy, fostering open discussions crucial for obtaining valuable qualitative data.

Interviewee ID	Role/Position
Interviewee 1	Director in a security Agency and responsible for privacy
Interviewee 2	Assistant Undersecretary in the government, responsible for bringing the cloud to Qatar
Interviewee 3	Director of Cloud Computing in Qatar
Interviewee 4	Associate Professor and Associate Dean for Academic Affairs
Interviewee 5	Associate Professor and Head of Information and Computing Technology
Interviewee 6	Advisor for Microsoft and Google cloud service providers in Qatar

Table 5. Participants' Information

3.3. Literature Search Strategy

For the literature search, Scopus and Google Scholar were utilized due to their comprehensive coverage of cloud computing and data sovereignty research. Scopus provided peer-reviewed academic papers with a focus on abstracts, titles, and keywords, while Google Scholar included broader sources such as government reports and think tank publications. Search terms like "Data Sovereignty," "Cloud Computing," "Qatar," and "Legislation" targeted the study's focus on Qatar's cloud infrastructure. The review spanned publications from 2010 to 2023, ensuring a thorough examination of both historical and recent developments in the field.

The Khatri and Brown (2010, 23) Data Governance Framework provides a practical view of data management tools and procedures. Data security, usability, and correctness require robust rules, norms, and processes in the cloud's dynamic and growing environment. Qataris must grasp these governance regimes to establish, contest, or reinterpret data sovereignty as more people use cloud platforms. This paper uses these theoretical approaches to analyse how technology and governance affect Qatar's cloud data privacy. Technological Determinism explains how cloud advancements change and the Data Governance Framework evaluates data sovereignty. This paper examines how Qatar might use and govern cloud computing. Data governance, new technology, and legal frameworks are analysed from two angles. Qatar and the world need multidimensional research on cloud computing[75]. This article addresses government, nationalism, and safety challenges many countries have with cloud computers. Independent state conflicts complicate problems. Abraham et al. (2019, 45) state that the research's findings and implications globally affect business and academic personnel. Looking at data governance and technology change together shows their cross-border connections.

3.2. Interviews

This paper explores how legislation and technology impact cloud computing in Qatar through structured interviews with key government, corporate, and academic figures. Insights from these interviews were analysed using Braun and Clarke's[76] thematic analysis, revealing critical data patterns and scholarly concepts. The research adhered strictly to Institutional Review Board (IRB) guidelines, ensuring ethical integrity. Informed consent, confidentiality, and participant protection were prioritized throughout the study, ensuring that the research was conducted with the highest ethical standards at Hamad Bin Khalifa University (HBKU).

3.2.1. Participant Selection

This paper used purposeful sampling to gather diverse perspectives on Qatari cloud computing, focusing on the complexities of data governance and policy. Participants were selected based on their senior positions, expertise in IT, data governance, and policy-making, ensuring informed insights into data sovereignty. The sample included professionals with extensive experience in cloud data governance, recognized thought leaders contributing to the field, and individuals from government, academia, tech, and cybersecurity sectors. This approach aimed

(75) P. Albrecht, "How the General Data Protection Regulation Will Change Our World," Journal of Privacy and Data Protection 2, no. 2 (2016): 84–90.

(76) V. Braun and V. Clarke, "Using Thematic Analysis in Psychology," Qualitative Research in Psychology 3, no. 2 (2006): 77–101.

fill these gaps by providing a nuanced understanding of cloud computing in the Qatari public sector, focusing on leadership's role in ensuring both technological innovation and regulatory compliance.

3. Methodology

Information security is crucial in Qatar's ever-changing digital environment[74]. This paper examines Qatar's legislative and technological criteria for moving from public to autonomous cloud infrastructure. As indicated by earlier research, it places data sovereignty in its proper place in Qatar and stresses its importance during a broad digitisation period.

3.1. Theoretical Framework

This study applies the Data Governance Framework and Technological Determinism to explore Qatar's cloud data sovereignty. Smith and Marx's (1994, 12) concept of Technological Determinism explains how technological advancements drive societal change, impacting government operations and data security in Qatar's IT sector.

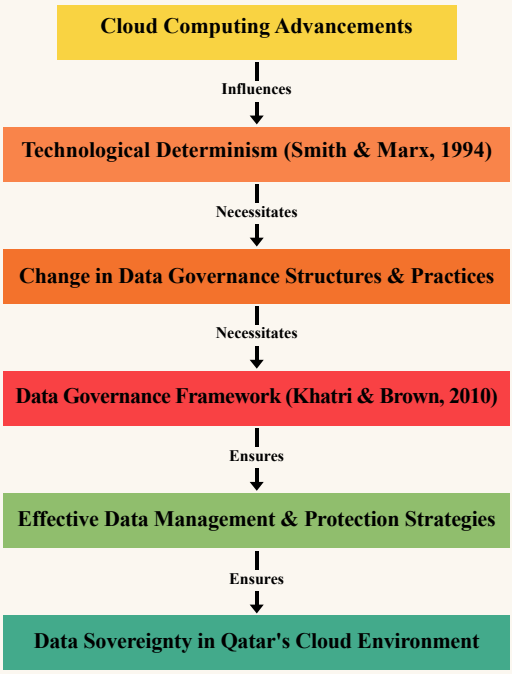


Figure 1: Theoretical Framework (Self-Created)

(74) K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS) (National Institute of Standards and Technology, 2007).

autonomy underscores the importance of integrating robust cloud data control strategies in Qatar[64]. Flexible access controls based on trust and reputation, as suggested by Yan et al.[65], could enhance data privacy in Qatar's cloud services. Additionally, encryption-based solutions, as discussed by Esposito et al.[66], are crucial for secure data migration across federated clouds—a key consideration for Qatar's collaboration with international cloud providers.

2.6. Gaps in Current Literature

Despite the wealth of literature on cloud computing and data sovereignty, existing research tends to emphasize technical advancements without fully addressing the socio-political and legal complexities of data management across jurisdictions. Studies like Zissis and Lekkas[67] and Marston et al.[68] provide foundational insights into the evolution of cloud computing, but they lack critical engagement with emerging challenges such as data localization and compliance in rapidly digitizing economies like Qatar. While Banse[69] discusses the complexities of open cloud ecosystems under the GDPR, there is limited exploration of how non-EU nations like Qatar adapt these frameworks to fit local legal and cultural contexts. Similarly, Giese and Anderl[70] offer solutions for secure data sharing but fail to address how these approaches can be scaled to governmental applications where data sovereignty is paramount. Furthermore, many referenced studies, including Rehman and Sakr[71] and Irion[72], are outdated and fail to account for recent advancements in cloud security technologies, such as AI-driven encryption systems[73]. This study aims to

(64) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(65) Z. Yan et al., "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing," IEEE Transactions on Cloud Computing 5, no. 3 (2015): 485–498.

(66) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds," IEEE Cloud Computing 3, no. 1 (2016): 12–17.

(67) D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems 28, no. 3 (2012): 583–592.

(68) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

(69) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(70) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(71) M. S. Rehman and M. F. Sakr, "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar," in 2011 IEEE Global Engineering Education Conference (EDUCON) (2011): 875–879.

(72) K. Irion, "Government Cloud Computing and National Data Sovereignty," Policy & Internet 4, no. 3-4 (2012): 40–71.

(73) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated Clouds," IEEE Cloud Computing 3, no. 1 (2016): 12–17.

practices, including clear geolocation rules, is crucial. Peterson et al.(62) emphasize knowing data storage locations to meet legal obligations, which is particularly important in Qatar.

Best Practice/Solution	Description	Reference
Data Localization	Storing data within the physical borders of a country to comply with local data protection laws.	Peterson et al., 2011
Encryption Technologies	Using encryption methods to secure data in transit and at rest, including techniques like homomorphic encryption.	Yu, Wang, Ren, & Lou, 2010
Access Control Mechanisms	Implementing strong access control policies, including attribute-based access control (ABAC) and role-based access control (RBAC).	Banse, 2021
Cloud Service Agreements	Ensuring cloud service agreements outline data handling, privacy, and compliance measures.	Wei et al., 2014
Auditing and Compliance Monitoring	Regular audits and monitoring for compliance with data protection laws and standards.	Hashem et al., 2015
Data Masking and Tokenization	Using data masking and tokenisation techniques to anonymise sensitive data.	Giese & Anderl, 2022
Federated Identity Management	Managing user identities and access across different cloud services and platforms.	Harauz et al., 2009
Cloud Data Management Interface (CDMI)	Standardising cloud storage and data management operations through CDMI protocols.	Sookhak et al., 2017
Hybrid Cloud Models	Combining private and public cloud models to optimise control and scalability.	Zissis & Lekkas, 2012
Trust and Reputation Management Systems	It establishes trust and reputation systems for evaluating the reliability of cloud services.	Yan et al., 2017

Table 4. Best Practices & Solutions

Implementing data governance, access, and usage management in shared data networks is complex, particularly in ensuring data sovereignty. Hellmeier et al.(63) highlight the need for clear data ownership and control, essential for Qatar's expanding digital projects. The impact of the EU's GDPR and EUCS on data

(62) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(63) M. Hellmeier et al., "Implementing Data Sovereignty: Requirements and Challenges from Practice," in Proceedings of the 18th International Conference on Availability, Reliability and Security (2023): 1–9.

the cloud security architecture is crucial. Safe cloud architectures require systems that handle data breaches, unauthorised access, and other cyber threats[55]. Due to foreign data protection laws, cloud data management is more complex. Like the GDPR, these laws restrict data handling, processing, and storage. To comply with these laws, cloud providers must adapt their operations[56]. Many things can go wrong when trying to secure cloud data. This includes addressing data leaks, unauthorised access, and user privacy violations. Several investigations into these threats have led to ways to protect data and privacy in untrustworthy cloud settings[57].

New technologies like flexible multi-keyword query techniques may solve current issues. These methods consider keyword weights and user access records when querying. This improves encrypted cloud data searching[58]. Cloud computing security involves legal and moral issues. Building cloud service trust requires considering these concerns. Secure and private cloud data is crucial for cloud computing and associated technologies[59]. Virtual product development could benefit from a new data ownership model that makes sharing and storage safer. This paradigm displays where distributed and preserved design data is and allows data owners to regulate access[60]. Data safety in cloud computing depends on numerous factors, including where data is held and enterprises' and service providers' legal requirements. Research[61] recommend explicit policy and governance frameworks for good cloud security. To conclude, cloud computing data privacy technologies are numerous. Encryption, data localisation, safe data storage, trust management, key management, and legal compliance is complex. Each aspect is crucial for cloud data security, privacy, and control.

2.5. Best Practices and Solutions

Global best practices ensure cloud data security and compliance with local laws. For Qatar, prioritizing digital transformation and data governance, adopting these

Clouds," IEEE Cloud Computing 3, no. 1 (2016): 12–17.

(55) Y. Sun et al., "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.

(56) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(57) J. Tang et al., "Ensuring Security and Privacy Preservation for Cloud Data Services," ACM Computing Surveys (CSUR) 49, no. 1 (2016): 1–39.

(58) K. Singi et al., "Data Sovereignty Governance Framework," in Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops (2020): 303–306.

(59) D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems 28, no. 3 (2012): 583–592.

(60) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(61) S. Medawar, "Information Retrieval in Systematic Reviews: Challenges and Opportunities," Information Processing & Management 58, no. 1 (2021): 102389.

locally can follow local data protection laws. The inherent nature of cloud computing, distributing data across multiple servers, introduces complex security challenges. For instance, the traditional approach of securing data in a localised data centre may lead to inefficiencies in a cloud environment, as it necessitates additional layers of security for data stored across various locations. This often results in increased costs and management complexity. A notable example is the need for advanced encryption methods during data transmission and at rest. Furthermore, it's essential to develop robust protocols for updating, deleting, and appending data in the cloud to mitigate risks of unauthorised access or data breaches(47). These measures are critical for maintaining data integrity and security in the cloud(48). Data storage security remains crucial with cloud computers. Plans are needed to protect distributed cloud data. To solve these issues, safer update, delete, and append methods are required(49).

Secure multi-party computation is crucial in collaborative cloud settings. It involves creating rules that allow many persons to compute a function over their inputs while keeping them hidden. This strategy is ideal for cloud environments where numerous parties exchange data and computing tools(50). Privacy and security of cloud data are crucial. For confidentiality, searchable encryption lets users seek encrypted cloud data without knowing what's inside(51). Cloud trust management systems are growing in popularity. These technologies evaluate cloud service reliability so users may make sensible data-sharing and storage decisions. Cloud environments are safer when data management is trusted(52). Effective cloud cryptographic key management is another interest. Key distribution, storage, and revocation must be secure to prevent theft(53).

Proxy re-encryption is a new, complex technology gaining popularity. It permits protected data to be switched encryption keys without revealing its content. This strategy is ideal for secure data sharing(54). In addition to these specialist technologies,

(47) C. Wang et al., "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transactions on Parallel and Distributed Systems 22, no. 5 (2010): 847–859.

(48) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(49) C. Wang et al., "Ensuring Data Storage Security in Cloud Computing," in 2009 17th International Workshop on Quality of Service (2009): 1–9.

(50) Y. Li et al., "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing," Information Sciences 387 (2017): 103–115.

(51) R. Li et al., "Efficient Multi-Keyword Ranked Query over Encrypted Data in Cloud Computing," Future Generation Computer Systems 30 (2014): 179–190.

(52) Z. Yan et al., "Flexible Data Access Control Based on Trust and Reputation in Cloud Computing," IEEE Transactions on Cloud Computing 5, no. 3 (2015): 485–498.

(53) S. K. Sood, "A Combined Approach to Ensure Data Security in Cloud Computing," Journal of Network and Computer Applications 35, no. 6 (2012): 1831–1838.

(54) C. Esposito, A. Castiglione, and K. K. R. Choo, "Encryption-Based Solution for Data Sovereignty in Federated

Regulation/Law	Description and Objective	Governing Body or Authority
Qatar Personal Data Protection Law (Law No. 13 of 2016)	It focuses on protecting personal data, regulates data processing activities, and ensures individuals' rights regarding their data.	National Cyber Security Agency (NCSA)
Qatar Cybercrime Prevention Law (Law No. 14 of 2014)	Addresses offences committed through information networks or computers, including unauthorised access, data breaches, and cyberattacks.	Ministry of Interior
Law No. (34) of 2006 on Electronic Commerce and Transactions	Establishes the legal framework for electronic transactions and e-commerce, including data authenticity and security measures.	Ministry of Commerce and Industry
Qatar Central Bank's Circulars on Electronic Payments	Regulates electronic payments, emphasises data security standards, and governs financial transactions through digital platforms.	Qatar Central Bank
National Information Assurance Policy (Data Classification)	Sets out policies and standards for information security in public and private sectors, aiming to protect against cyber threats and data breaches.	National Cyber Security Agency (NCSA)
Qatar Cloud Policy Framework	Provides guidelines and principles for cloud adoption in government and semi-government entities, focusing on data sovereignty and security.	Ministry of Transport and Communications

Table 3. Laws and Regulations Governing Data Sovereignty in Qatar

2.4. Technological Perspectives

Cloud computing makes data sovereignty difficult and requires new technologies and strategies. Many solutions in the literature address different data sovereignty issues. These solutions include best practices for encryption, data localisation, and cloud data sharing. One of the best ways to protect cloud data is encryption. Attribute-based encryption (ABE) is a significant advancement in this sector since it lets you restrict data access based on user characteristics. Complex cloud access rules are best enforced using this strategy(45). Homomorphic encryption allows the handling of encrypted data without revealing its contents, thereby protecting data privacy(46). Data privacy is increasingly protected via localisation. Businesses that keep data

(45) S. Yu et al., "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," in 2010 Proceedings IEEE INFOCOM (2010): 1–9.

(46) K. Shatilov et al., "Solution for Secure Private Data Storage in a Cloud," in 2014 Federated Conference on Computer Science and Information Systems (2014): 885–889.

strict responsibilities on data controllers and processors while enhancing individual rights[40][41]. The GDPR's extraterritorial reach means that organizations outside the EU, including those in Qatar, must comply when handling EU residents' data, raising complex sovereignty issues[42]. In Qatar, the GDPR's relevance is twofold: Qatari organizations dealing with EU data must align with GDPR standards, necessitating an international compliance strategy. Additionally, Qatar's Personal Data Protection Law, inspired by the GDPR, reflects the nation's commitment to high data protection standards. However, balancing local laws with international regulations presents challenges, particularly in ensuring compliance while navigating global data protection complexities. The importance of geolocating cloud data is emphasized by Peterson et al.[43], who highlight the legal and policy challenges when data is virtualized and distributed globally. Qatar's proactive approach to cloud computing and data security, especially in government services, underscores its commitment to maintaining data sovereignty while engaging with the global digital economy[44].

Period	Regulatory Framework	Key Features	Impact on Cloud Computing
The early 2000s	Data Protection Directive (EU)	Protection of personal data and privacy.	Increased awareness of data privacy and sovereignty.
2008-2010	Health Information Technology for Economic and Clinical Health (HITECH) Act (USA)	Enhanced data protection for health information.	Heightened focus on securing health-related data in the cloud.
2012	General Data Protection Regulation (GDPR) Proposal (EU)	Comprehensive data protection regulation, including data sovereignty.	A significant shift in cloud data management and compliance requirements.
2016	GDPR Enforcement (EU)	Strict data protection and privacy standards; heavy fines for non-compliance.	Significant impact on cloud service providers; focus on data localisation and sovereignty.
2018	California Consumer Privacy Act (CCPA) (USA)	Similar to GDPR, it focuses on consumer privacy rights.	Influencing cloud computing policies and practices in the USA.
2020s	Emergence of National Data Protection Laws (Global)	Countries worldwide enacting data protection laws, influencing cloud computing practices.	Global cloud services adapting to diverse national regulations.

Table 2. Regulatory Framework

(40) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(41) N. J. King and V. T. Raja, "Protecting the Privacy and Security of Sensitive Customer Data in the Cloud," Computer Law & Security Review 28, no. 3 (2012): 308–319.

(42) A. Kronabeter and S. Fenz, "Cloud Security and Privacy in the Light of the 2012 EU Data Protection Regulation," in Cloud Computing: Third International Conference, CloudComp 2012, Vienna, Austria, September 24-26, 2012, Revised Selected Papers, 3 (Springer International Publishing, 2013): 114–123.

(43) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(44) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

2.2. Data Sovereignty in Cloud Computing

Cloud computing "data sovereignty" has become a critical area of study due to the growing complexity of managing data across jurisdictions. This literature review explores global data sovereignty, with a particular focus on Qatar. Data sovereignty refers to the legal and practical control over data stored in the cloud. Peterson et al.[35] highlight the challenges of establishing control over virtualized and globally distributed data, which is complicated by decentralized cloud services. This is especially problematic in maintaining data within the correct legal jurisdiction.

Banse[36] discusses how the EU General Data Protection Regulation (GDPR), the European Cybersecurity Certification Scheme for Cloud Services (EUCS), and Gaia-X complicate data privacy in open cloud ecosystems. While protected enclaves and encrypted virtual machine memory offer new ways to safeguard data, they do not fully secure the system. Giese and Anderl[37] emphasize the importance of secure data sharing for virtual product development, particularly in controlling dispersed data in cloud environments. Sun et al.[38] examine software and hardware security challenges in cloud computing, underscoring the need for robust privacy measures. Irion[39] discusses data sovereignty in government cloud services, highlighting legal risks that technology and contracts alone cannot mitigate. Qatar, with its evolving technology and strict data control standards, must balance global technological standards with its own legal frameworks to manage cloud computing data sovereignty effectively.

2.3. Regulatory and Legal Framework

As digital data increasingly crosses borders, cloud computing data sovereignty regulations have become crucial. These frameworks address the complex legal, ethical, and technical challenges of storing and processing data in a global, decentralized cloud environment. The European Union's General Data Protection Regulation (GDPR) has significantly transformed global data protection standards, imposing

(35) Z. N. J. Peterson, M. Gondree, and R. Beverly, "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud," in Proceedings of the 3rd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud '11) (2011).

(36) C. Banse, "Data Sovereignty in the Cloud—Wishful Thinking or Reality?" in Proceedings of the 2021 on Cloud Computing Security Workshop (2021): 153–154.

(37) T. Giese and R. Anderl, "Maintaining Control over Distributed Data through a Data Sovereignty Model," in 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA) (2022): 1–7.

(38) Y. Sun et al., "Data Security and Privacy in Cloud Computing," International Journal of Distributed Sensor Networks 10, no. 7 (2014): 190903.

(39) K. Irion, "Government Cloud Computing and National Data Sovereignty," Policy & Internet 4, no. 3-4 (2012): 40–71.

goals, is anchored in strategic vision, with investments in cutting-edge data centres and global tech partnerships[32].

Period	Key Developments	Significant Contributors	References
1960s-1970s	Concept of utility computing by John McCarthy; early forms of shared resource computing.	John McCarthy and others in the field of shared computing.	Peterson et al., 2011
1980s-1990s	The emergence of grid computing; early Internet-based computing developments.	Development of grid computing concepts by various researchers and technologists.	Zissis & Lekkas, 2012
The early 2000s	Cloud computing begins to take shape with the introduction of AWS, enabling more comprehensive access to computing resources.	Amazon Web Services (AWS) and other early cloud service providers.	Zhang et al., 2010
Late 2000s-2010s	Rapid expansion of cloud services; introduction of major platforms like AWS, Azure, and Google Cloud.	Major tech companies like Amazon, Microsoft, and Google are developing and expanding cloud platforms.	Marston et al., 2011; Biocic et al., 2011
2010s-Present	Advancements in cloud technology are increasing the focus on data sovereignty, privacy, security, and GDPR implementation.	Global policymakers, technologists, and organisations focusing on data security and sovereignty laws.	Banse, 2021; Giese & Anderl, 2022

Table 1. Evolution of Cloud Computing

Qatar's adoption of cloud computing has enhanced service delivery and spurred innovation[33], yet it faces significant challenges, particularly in data privacy and security. These challenges are unique due to the need to align rapidly evolving cloud technologies with Qatar's specific legal and cultural frameworks, such as the Qatar Personal Data Protection Law. Cloud computing has revolutionized IT, driving economic and strategic shifts globally[34]. In Qatar, this transformation is further complicated by the need to balance digital advancement with stringent data protection and cultural sensitivities.

(32) M. S. Rehman and M. F. Sakr, "Teaching the Cloud: Experiences in Designing and Teaching an Undergraduate-Level Course in Cloud Computing at Carnegie Mellon University in Qatar," in 2011 IEEE Global Engineering Education Conference (EDUCON) (2011): 875–879.

(33) N. Sultan, "Cloud Computing: A Democratising Force?" International Journal of Information Management 33, no. 5 (2013): 810–815.

(34) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

public sector to ensure compliance with both national and international data protection and privacy laws, particularly in the context of cross-border data flows enabled by cloud services.

The study will demonstrate how Qatar's government can use cloud computing to boost operational efficiency, data privacy, and digital transformation leadership. This study offers valuable insights for Qatari policymakers, public administrators, and IT leaders by analysing government cloud technology adoption. It highlights how public institutions can improve efficiency, security, and compliance with data sovereignty. The study provides a roadmap for balancing global cloud benefits with data sovereignty, aligning with Qatar's National Vision 2030, and offers recommendations for effective leadership and ICT integration in the public sector[24][25][26].

2. Literature Review

2.1. Evolution of Cloud Computing

The global rise of cloud computing, including in Qatar, marks a transformative shift in information technology, characterized by significant advancements and unique adaptations to meet evolving demands. This literature review explores cloud computing's evolution and Qatar's distinctive journey. Cloud computing originated from mainframes and evolved through grid and utility computing[27], transitioning from traditional on-premises IT to scalable, service-focused models. Zhang et al. [28]highlight how cloud computing minimizes the need for extensive hardware, enabling on-demand services. This shift has revolutionized business paradigms across industries[29], facilitating flexible, pay-as-you-go services[30]. Mishra et al.[31] discuss the importance of speed, scalability, and availability in public and multi-cloud systems. Qatar's cloud computing strategy, aligned with its ambitious digitalization

(24) P. Banerjee, "Governing the Cloud: Policy Strategies for Data Sovereignty and Digital Infrastructure," Digital Policy, Regulation and Governance 24, no. 2 (2022): 125–137.

(25) Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," Journal of Internet Services and Applications 1 (2010): 7–18.

(26) X. Zhu, H. Liu, and S. Wei, "Cloud Computing Adoption in the Public Sector: A Meta-Analysis of Antecedents and Outcomes," Information Systems Frontiers 23, no. 5 (2021): 1229–1248.

(27) D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems 28, no. 3 (2012): 583–592.

(28) Q. Zhang, L. Cheng, and R. Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges," Journal of Internet Services and Applications 1 (2010): 7–18.

(29) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

(30) B. Biočić, D. Tomić, and D. Ogrizović, "Economics of Cloud Computing," in 2011 Proceedings of the 34th International Convention MIPRO (2011): 1438–1442.

(31) M. Mishra et al., "An Assessment of Cloud Computing: Evolution," Journal of Cloud Computing: Advances, Systems and Applications, 2020.

how public investment can enhance cloud computing while safeguarding data sovereignty. These strategies provide a model for countries with similar challenges, helping to shape policies that integrate legal, economic, and cybersecurity measures effectively(22). While cloud computing has been increasingly adopted by the public sector, there remains a significant gap in understanding how leadership styles influence the successful adoption and implementation of cloud technologies, particularly in regions like Qatar where digital transformation is driven by national strategies such as Qatar National Vision 2030. Current literature primarily focuses on technical aspects of cloud computing or general policy implications(23), but fails to explore the role of leadership in this transformation. This study aims to fill this gap by examining how different leadership styles within Qatari public sector organizations impact cloud adoption, data sovereignty, and public service delivery. Specifically, the research seeks to explore the strategic decisions leaders make, their approach to managing change, and how they foster collaboration with cloud service providers. This is crucial for understanding how leadership can drive innovation in public administration, and how such insights can be applied globally in similar contexts. By addressing this gap, the study contributes to the growing body of knowledge on public sector modernization and digital governance, providing a nuanced understanding of the leadership challenges and opportunities in cloud computing adoption.

Research Question

How does the adoption of cloud computing in Qatar's public sector influence leadership styles and data sovereignty while ensuring compliance with national and international regulations?

Revised Research Objectives:

1. **To Identify Key Leadership Traits:** Analyse specific leadership traits and decision-making strategies that facilitate the successful adoption and management of cloud computing in Qatar's public sector, focusing on their role in overcoming implementation challenges.
2. **To Evaluate the Impact of Cloud Computing on Data Sovereignty:** Assess how cloud computing adoption impacts Qatar's data sovereignty, specifically examining the balance between utilizing global cloud services and adhering to national data privacy laws and international regulations.
3. **To Explore Compliance Strategies:** Investigate the strategies used by Qatar's

(22) S. Chakraborty and K. Joseph, ICT and Digital Transformation in the Middle East (Routledge, 2021).
(23) Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework," Journal of Enterprise Information Management 26, no. 3 (2013): 250–275

practices crucial for cloud computing adoption. The study examines how Qatari leaders navigate these dynamics, emphasizing strategic foresight, risk management, innovation, and compliance. Given that leadership drives digital transformation[14], integrating cloud technologies into public administration supports Qatar's knowledge-based economy. This research highlights the importance of change management, stakeholder engagement, and ethics, showing that effective leadership is key to enhancing public sector productivity through cloud computing[15].

This study also shows how leadership styles affect cloud computing resource management and strategic partnerships with cloud service providers. Leaders can improve service agreements, adapt to new technologies, and use outside experts better[16]. This collaborative leadership style is ideal for Qatari public sector organisations that hire foreign cloud service providers to set up and run their digital infrastructures. Qatar National Vision 2030 (QNV 2030) calls for a digital transformation, making it a good place to study cloud computing and data sovereignty. QNV 2030 aims to make Qatar a knowledge-based economy by 2030. This change will heavily involve ICTs. Qatar has invested heavily in digital infrastructure, including the Qatar Smart Program. Cloud computing improves public services and diversifies the economy[17]. Qatar's legal system blends Islamic and modern law. This makes data sovereignty discussions unique. The Personal Data Privacy Protection Law No. 13 of 2016 establishes a comprehensive data protection system similar to the EU's General Data Protection Regulation (GDPR) but tailored to Qatar's legal and cultural norms[18]. This dual legal system alters data sovereignty and makes it harder to enforce national and international laws[19].

This case study extends beyond Qatar, offering insights for nations balancing data sovereignty with global cloud services. Qatar's experience aids in managing cross-border data flows, establishing compliance, and negotiating international agreements[20]. This is vital for MENA markets with diverse legal systems[21]. Qatar's government-led digital transformation, supported by the QNV 2030, exemplifies

(14) J. D. Houghton, A. Carnes, and C. N. Ellison, "A Cross-Sectional Examination of Transformational Leadership and Transformational Leaders in the United States," Leadership Quarterly 26, no. 3 (2015): 437–447.

(15) I. Nurdiani, M. S. Börjesson, and L. Angelis, "A Systematic Mapping Study on the Combination of Agile Software Development and Leadership Styles," Journal of Systems and Software 161 (2020): 110459.

(16) R. Heeks and C. Stanforth, "Technological Change in Developing Countries: Opening the Black Box of Process Using Actor-Network Theory," Development Studies Research 2, no. 1 (2015): 33–50.

(17) Ministry of Transport and Communications, Qatar Smart Program (TASMU) (Ministry of Transport and Communications, 2019).

(18) Qatar Financial Centre, Personal Data Privacy Protection Law No. 13 of 2016 (Qatar Financial Centre, 2020).

(19) Baker McKenzie, "Qatar: Data Protection Overview," Baker McKenzie, 2021.

(20) M. Al-Naama, "Data Sovereignty in the GCC: Legal and Regulatory Perspectives," Gulf Affairs, 2022.

(21) GCC-STAT, GCC Statistical Centre: Data Sovereignty and Cloud Computing (GCC-STAT, 2022).

As governments worldwide transition towards post-industrial infrastructures to meet rising citizen demands and the need for transparency and productivity, cloud computing emerges as a timely, cutting-edge research topic[9]. Modern public sector operations require a significant amount of data, and cloud computing provides the elasticity to host and store it. It simplifies data processing, thereby improving digital governance and decision-making. The cloud allows public sector entities to store and process data from the internet rather than on a local server, providing real-time information to inform policy decisions that enhance public service delivery[10]. This capability aids smart governance by enabling data-driven systems to better manage urban infrastructure and services[11].

The study meets the International Journal of Public Administration and Digital Administration (IJPADA) scope of innovative public sector management practices. The journal prioritises digital tools in public administration, particularly how they can improve governance (IJPADA n.d., 5). This paper explores the many uses of cloud computing in public sector management to improve administrative processes and service delivery. It examines public sector cloud adoption opportunities and challenges, including data security, privacy, and regulatory compliance. This mixed-method study examined cloud-based solutions' security and deployment challenges for public sector organisations[12]. It addresses IJPADA's digital transformation challenges in public administration and provides a deeper understanding of ICTs' barriers to IOS participation. This research also examines cloud computing's impact on public sector efficiency beyond IT, using case studies to show best practices and lessons learned. The study examines real-world applications and offers policymakers practical insights into digital service transformation[13].

This study uniquely explores leadership styles in Qatari public sector cloud adoption, addressing a gap in research typically focused on technology and policy. Cloud leadership involves strategic vision, decision-making, and management

Maturity, Capabilities, and Data Portfolios," Government Information Quarterly 31, no. 3 (2014): S57–S68.

(9) V. Weerakkody, M. Janssen, and Y. K. Dwivedi, "Transformational Change and Business Process Reengineering (BPR): Lessons from the British and Dutch Public Sector," Government Information Quarterly 28, no. 1 (2016): 27–36.

(10) J. R. Gil-Garcia, N. Helbig, and A. Ojo, "Being Smart: Emerging Technologies and Innovation in the Public Sector," Government Information Quarterly 31, no. S1 (2014): S2–S8.

(11) T. Nam and T. A. Pardo, "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions," in Proceedings of the 12th Annual International Conference on Digital Government Research (2011): 282–291.

(12) M. Almorsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem," Communications of the ACM 59, no. 1 (2016): 38–46.

(13) A. Cordella and N. Tempini, "E-Government and Organizational Change: Reappraising the Role of ICT and Bureaucracy in Public Service Delivery," Government Information Quarterly 32, no. 3 (2015): 279–286.

1. Introduction

ICTs have transformed almost all sectors, especially the public sector, which uses them to improve efficiency, transparency, and service delivery. ICTs have enabled e-government, which is more efficient, resource-efficient, and public-engaged(1). This transformation is essential for the public sector to respond quickly to societal needs and increase access to digital tools in front-end services and data(2). Cloud computing has become essential to ICTs, providing scalable and flexible solutions to meet changing public administration needs. Cloud computing allows online data storage, processing, and management without servers or hardware(3). This savings helps public sector organizations deliver services cheaper, faster, and more agilely(4). Cloud computing has the potential to revolutionize public administration through data-driven decision-making and service innovation. Cloud technologies enable government departments to share data and collaborate, thereby enhancing integrated service delivery and operational efficiency(5). Data is not just important, it's crucial for urban management and policy applications in smart cities and digital governance(6). Local laws ensure the protection of sensitive government data, meeting national security and data sovereignty requirements in the public sector(7). A comprehensive understanding of the cloud is essential to meet administrative and citizen demands in this digital age. In the following paragraphs, we will delve into how cloud computing fits into public sector modernization using Qatari study case data, and how data-driven decision-making is shaping the future of public policies.

The study examines public sector ICT use, with a specific focus on the transformative role of cloud computing. The digitalisation of public services has led to a cloud-based approach to scaling and flexing IT resources. This is crucial for public administrations to enhance service delivery, citizen engagement, and efficiency(8).

(1) J. C. Bertot, P. T. Jaeger, and J. M. Grimes, "Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies," Government Information Quarterly 27, no. 3 (2010): 264–271.

(2) F. Bannister and R. Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research," Government Information Quarterly 31, no. 1 (2014): 119–128.

(3) S. Marston et al., "Cloud Computing—The Business Perspective," Decision Support Systems 51, no. 1 (2011): 176–189.

(4) Y. Alshamaila, S. Papagiannidis, and F. Li, "Cloud Computing Adoption by SMEs in the North East of England: A Multi-Perspective Framework," Journal of Enterprise Information Management 26, no. 3 (2013): 250–275

(5) A. Chandrasekaran and M. Kapoor, "State of the Public Cloud: The Cloud Adoption Conundrum," Infosys Labs Briefings 9, no. 1 (2011): 3–10.

(6) T. Clohessy, T. Acton, and L. Morgan, "Smart City as a Service (SCaaS): A Future Roadmap for E-Government Smart City Cloud Computing Initiatives," Digital Policy, Regulation and Governance 19, no. 1 (2017): 58–69.

(7) H. Yang and M. Tate, "A Descriptive Literature Review and Classification of Cloud Computing Research," Communications of the Association for Information Systems 31, no. 1 (2012): 2–57.

(8) M. Janssen, E. Estevez, and T. Janowski, "Interoperability in Big, Open, and Linked Data–Organizational

المُلخَّص

سيادة البيانات على الحوسبة السحابية: دراسة لبيئة الحوسبة السحابية في دولة قطر

عبدالرحمن محمد آل شافي
مدير إدارة الاستراتيجيات والسياسات السيبرانية – الوكالة الوطنية للأمن السيبراني

يستكشف هذا المشروع البحثي المشهد المتطور لسيادة البيانات السحابية في قطر، ويفحص التفاعل الديناميكي بين التقدم التكنولوجي والأطر القانونية. تركز الدراسة على فهم الجوانب الحاسمة لسيادة البيانات في الحوسبة السحابية، وخاصة في ظل البنية التحتية الرقمية سريعة التطور في قطر. باستخدام نهج الأساليب المختلطة، يدمج البحث بعض من المقابلات النوعية مع خبراء الصناعة والأكاديميين الرئيسيين إلى جانب مراجعة شاملة لـ 15 دراسة ذات صلة.

يستكشف الجزء النوعي وجهات نظر مباشرة من المسؤولين الحكوميين والخبراء القانونيين ومحترفي التكنولوجيا، ويكشف عن موضوعات حول توطين البيانات والامتثال التنظيمي والفروق الدقيقة المميزة لبيئات السحابة الخاصة مقابل العامة. تكمل مراجعة الأدبيات هذه من خلال توفير فهم أوسع للاتجاهات العالمية ووضع تحديات وفرص قطر الفريدة في سياق سيناريو الحوسبة السحابية العالمية.

تكشف النتائج عن نسيج معقد من القضايا، بدءًا من التحديات التنظيمية ومخاوف الخصوصية إلى الآثار الاستراتيجية على الأمن القومي والتنمية الاقتصادية. تؤكد الدراسة على الحاجة إلى أطر قانونية وتنظيمية قوية في قطر للتنقل في عالم السيادة على البيانات السحابية المعقدة. كما يقدم توصيات عملية لصناع السياسات ومقدمي خدمات الحوسبة السحابية والمستخدمين النهائيين، بهدف تعزيز بيئة مواتية للابتكار التكنولوجي مع حماية سيادة البيانات. يساهم هذا المشروع في الحوار المستمر حول الحوسبة السحابية في قطر، مما يوفر فهمًا دقيقًا للتقاطع بين التكنولوجيا والقانون والسياسة في العصر الرقمي.

الكلمات المفتاحية: الحوسبة السحابية، سيادة البيانات، التحول الرقمي، الابتكار التكنولوجي، الأطر القانونية والتنظيمية، صناع السياسات.

Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar

Abdulrahman Mohammed M SH Al-Shafi
Masters of Public Policy (HBKU) - Director of Cyber Strategies and Policies Department
National Cyber Security Agency (NCSA)

ABSTRACT

This paper project delves into the evolving landscape of cloud data sovereignty in Qatar, scrutinizing the dynamic interplay between technological advancements and legal frameworks. The study focuses on understanding the critical aspects of data sovereignty in cloud computing, particularly under Qatar's rapidly developing digital infrastructure. Using a mixed-methods approach, the research incorporates insights from qualitative interviews with key industry and academic experts alongside a comprehensive review of 15 pertinent studies. The qualitative segment explores first-hand perspectives from government officials, legal experts, and technology professionals, uncovering themes around data localization, regulatory compliance, and the distinct nuances of private versus public cloud environments. The literature review supplements this by providing a broader understanding of global trends and contextualizing Qatar's unique challenges and opportunities within the global cloud computing scenario.

Findings reveal a complex tapestry of issues, ranging from regulatory challenges and privacy concerns to strategic implications for national security and economic development. The study underscores the need for robust legal and regulatory frameworks in Qatar to navigate the intricate world of cloud data sovereignty. It also offers practical recommendations for policymakers, cloud service providers, and end-users, aiming to foster an environment conducive to technological innovation while safeguarding data sovereignty. This paper contributes to the ongoing discourse on cloud computing in Qatar, providing a nuanced understanding of the intersection between technology, law, and policy in the digital age.

Keywords: Cloud Computing, Data Sovereignty, Digital Transformation, Technological Innovation, Legal and Regulatory Framework, Policymakers.

Data Sovereignty over the Cloud: An Examination of the Cloud Environment in Qatar

Abdulrahman Mohammed M SH Al-Shafi

Masters of Public Policy (HBKU) - Director of Cyber Strategies and Policies Department
National Cyber Security Agency (NCSA)

- Organization for Social Media Safety, (2021). Cyberbullying: 6 Reasons Why It's Common. https://www.socialmediasafety.org/blog/cyberbullying-6-reasons-why-its-common/
- Özdemir, S.A., Kuzucu Y. (2015). Cybervictimization and cyberbullying: the mediating role of anger, don't anger me! Comput Hum Behav. 49:437–443. doi:10.1016/j.chb.2015.03.03012.
- Patchin JW, Hinduja S. (2011). Traditional and nontraditional bullying among youth: a test of general strain theory. Youth Soc. 43 (2):727e751. doi:10.1177/0044118X1036695113.
- Reyhani, N.,(2015). A Critical Examination of Educational Policies Designed to Combat Cyberbullying Among Youth. A Major Paper Presented to the Political Science Department of the University of Guelph Department In partial fulfillment of the Master of Arts degree. Canada
- Ruangnapakul, N., Salam, Y. D., & Shawkat, A., R., (2019). A Systematic Analysis of Cyber Bullying in Southeast Asia Countries. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, 8, (8S)
- Schonfeld, A., McNiel, D., Toyoshima, T., & Binder, R., (2023). Journal of the American Academy of Psychiatry and the Law Online February 2023, JAAPL.220078-22; DOI: https://doi.org/10.29158/JAAPL.220078-22
- Sela-Shayovitz R, Levy M, Hasson J.(2024). The Role of Self-Control in Cyberbullying Bystander Behavior. Social Sciences. 13(1):64. https://doi.org/10.3390/socsci13010064 . file:///C:/Users/HP/Downloads/socsci-13-00064-v4%20(2).pdf
- Werner, N. E., Bumpus, M. F., & Rock, D. (2010). Involvement in Internet aggression during early adolescence. Journal of Youth and Adolescence, 39, 607–619. doi:10.1007/s10964-009-9419-7
- Willard, N. (2005). Educator's guide to cyberbullying addressing the harm caused by online social cruelty. Scientific Research.

- Kraft E, Wang J. (2011). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to the victimization of students at a public liberal arts college. Int J Tech. 2011;1:74–91.7.
- Law DM, Shapka JD, Hymel S, Olson BF, Waterhouse T. (2011). The changing face of bullying: an empirical comparison between traditional and internet bullying and victimization. Comput Hum Behav. 2012;28(1):226–232. doi:10.1016/j.chb.2011.09.00437
- Linton DK, Power JL. (2013). The personality traits of workplace bullies are often shared by their victims: Is there a dark side to victims? Pers Individ Differ. 2013;54(6):738–743. doi:10.1016/j.paid.2012.11.02638
- Luo Q, Wu N, Huang L. (2023). Cybervictimization and cyberbullying among college students: The chain mediating effects of stress and rumination. Front Psychol. 14:1067165. doi: 10.3389/fpsyg.2023.1067165. PMID: 36844269; PMCID: PMC9950563.
- Maurya, C., Muhammad, T., Dhillon, P. et al. The effects of cyberbullying victimization on depression and suicidal ideation among adolescents and young adults: a three year cohort study from India. BMC Psychiatry 22, 599 (2022). https://doi.org/10.1186/s12888-022-04238-x https://bmcpsychiatry.biomedcentral.com/articles/10.1186/s12888-022-04238-x#Sec8
- Mcgrath L. H., (2017). Can the general theory of crime and general strain theory explain cyberbullying perpetration? Crime & Delinquency. 64(5):674–700. doi:10.1177/0011128717714204
- Mishna F, et al., (2016). The contribution of social support to children and adolescents self-perception: The mediating role of bullying victimization. Child Youth Serv Rev. 63:120–7.
- Mishna, F., Cook, C., Gadalla, T., Joanne, D., J & Solomon, S. (2010). Cyber Bullying Behaviors Among Middle and High School Students. American Journal of Orthopsychiatry. 80(3), 362–374
- Moon B., & Fifta L., Alarid (2015). School Bullying, Low Self-Control, and Opportunity. Journal of Interpersonal Violence 30(5) 839– 856
- National Council for Family Affairs (2021). Jordan stands together in the face of cyber bullying Great success for 'the new epidemic at the time of the pandemic' campaign. https://ncfa.org.jo/en/news/jordan-stands-together-in-the-face-of-cyber-bullying-great-success-for-the-new-epidemic-at-the-time-of-the-pandemic-campaign

- Alrawashdeh, M.N., Alsawalqa, R.O., Alnajdawi, A. et al. Workplace cyberbullying and social capital among Jordanian university academic staff: a cross-sectional study. Humanit Soc Sci Commun 11, 334 (2024). https://doi.org/10.1057/s41599-024-02805-z
- Al-Shatnawi FE, Ababneh AMT, Elemary FM, Rayan A, Baqeas MH. Prevalence of Cyberbullying Perpetration and Cyberbullying Victimization among Nursing Students in Jordan. SAGE Open Nurs. 2024 May 21;10:23779608241256509. doi: 10.1177/23779608241256509. PMID: 38784648; PMCID: PMC11113056.
- Chen D, Xu B, Chen J. (2023). The association between domestic violence exposure and cyberbullying behavior among secondary school students. Front Psychiatry. Dec 22;14:1302477. doi: 10.3389/fpsyt.2023.1302477. PMID: 38188055; PMCID: PMC10766691.
- Dou G, Xiang Y, Sun X, Chen L. (2020). Link Between Cyberbullying Victimization and Perpetration Among Undergraduates: Mediating Effects of Trait Anger and Moral Disengagement. Psychol Res Behav Manag ;13:1269-1276 https://doi.org/10.2147/PRBM.S286543
- Foody M, McGuire L, Kuldas S & O'Higgins, Norman J (2019). Friendship Quality and Gender Differences in Association with Cyberbullying Involvement and Psychological Well-Being. Front. Psychol. 10:1723. doi: 10.3389/fpsyg.2019.01723. file:///C:/Users/HP/Downloads/fpsyg-10-01723.pdf
- Gohal, G., Alqassim, A., Eltyeb, E. et al. (2023). Prevalence and related risks of cyberbullying and its effects on adolescents. BMC Psychiatry 23, 39 (2023). https://doi.org/10.1186/s12888-023-04542-0
- Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. Stanford, CA: Stanford University Press.
- Grasmick, H., Tittle, C., Bursik, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. Journal of Research in Crime & Delinquency, 30, 5-29.
- Hay, C., & Forrest, W. (2008). Self-control theory and the concept of opportunity: The case for a more systematic union. Criminology, pp. 1039–1072.
- Kamath P, Dsouza SM, Mahapatra S, et al. (2021). Prevalence of depression among school going adolescents in India: a systematic review and meta-analysis of cross-sectional studies. Int J Community Med Public Health. 8:833.
- Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: Bullying in the digital age (2nd ed)). Malden, MA: Wiley-Blackwell.

References

- Al-Badayneh, D (2023) Developing A College Students' Cyberbullying Scale. Open Access Journal of Criminology Investigation & Justice (OAJCIJ). https://medwinpublishers.com/OAJCIJ/developing-a-college-students-cyberbullying-scale.pdf
- Al-Badayneh, D. (2024). Prevalence, Viewpoints, and Encounters with Cyberterrorism among College Students. Journal of Ecohumanism.
- Al-badayneh, D. Al-Assasfeh, R. & Siddik Ekici (2023). Developing A Robust Legal System Through Scale for Youth Extremism Across Arab Cultures. International Journal of Criminal Justice Science Vol 18 Issue 1, 29-51
- Al-Badayneh, D., Al-Hagry, D., and Ben Brik, A., (2022), Cyberbullying, Victimization, Strains and Delinquency In Qatar. European Journal of Science and Theology, December 2022, Vol.18, No.6, 37-45
- Al-Badayneh, D., Al-Khattar, A. Al-Kresha R., and Al-Hassan, K.,(2012). Bullying victimization among college students (A transnational problem): A test of Agnew's General Strain Theory. The Homeland Security Review. Vol. 6, n2, 83-108.
- Al-Badayneh, D., Ben Brik, A., and Elwakad, A. (2023). A partial empirical test of the general strain theory on cyberbullying victimization among expatriate students. Journal Of Criminological Research, Policy And Practice. VOL. 10 NO. 1 2024, pp. 35-52. https://www.emerald.com/insight/content/doi/10.1108/JCRPP-03-2023-0013/full/html
- Al-Badayneh, D., Khelifa M. & Aladra, I., (2024). The Relationship Between Cyberbullying and Depression Among College Students . International Journal of Forensic Sciences (IJFSC).
- Al-Badayneh, D., Khelifa M. & Ben Brik, A. (2024). Cyberbullying and Cyberbullicide Ideation Among College Students International Journal of Cyber Criminology.
- Al-Badayneh, D.; And Al-Khuraisheh, Rafi' (2013). Criminology Theories: Introduction, Evaluation and Applications, First Edition, Dar Al Fikr Publishers and Distributors, Amman.
- Al-Darawsheh, A., Abutayeh, N., & Alrekebat, A.,(2021). Cyberbullying across youths in Jordan Community: Perspectives of the Faculty of Education students in Al-Hussein bin Talal University . Journal of Education and Practice www.iiste.org ISSN 2222-1735 (Paper) ISSN 2222-288X (Online) Vol.12, No.15, 2021 pp 62-74. https://www.researchgate.net/publication/352134868_Cyberbullying_across_youths_in_Jordan_Community_Perspectives_of_the_Faculty_of_Education_students_in_Al-Hussein_bin_Talal_University

5. Conclusion

Cyberbullying has gained global attention, it remins under-researched in Arab countries. Cyberbullying victimization is more common among females than males, whereas cyberbullying perpetrations are higher among males compared to females. In the future, victims of cyberbullying may become be perpetrators, and vice versa.

Cyberbullying risk factors include personality traits (low self-control), organizational settings, and social culture. Cyberbullying may result in serious health and legal consequences. The results suggest focusing on different mechanisms of self-control to prevent cyberbullying behaviors among secondary school students. Victims of cyberbullying require a variety of services and support, including but not limited to legal, health, and psychological assistance. This paper suggests more qualitative and quantitative research to validate cyberbullying in these countries and recommends data collection dates, definitions, and multiple-source reporting for better understanding (Ruangnapakul, Salam, & Shawkat, 2019). Policy formation, law enforcement, and preventive measures are necessary to combat cyberbullying.

6. Implications for higher education prevention

The widespread prevalence of cyberbullying on campus is concerning and should prompt the university administration to take action on all levels. This includes policy formation, lawmaking, preventive measures and victim programs. **Law enforcement** The trans-organizational nature of cyberbullying behavior necessitates law enforcement on university campuses and beyond. Breaking the law may occur on campus and spread outside.

The student awareness campaign is necessary to educate students about the criminal nature of cyberbullying and the severe consequences it can have on campus. A wide range of services are needed for on-campus victims of cyberbullying. Some psychological problems, such as depression, fear, loss of interest in life, suicidal ideation, and suicide, are prevalent among on-campus victims of cyberbullying. In addition to psychological and health help, victims also require legal assistance. Services should be significantly female-oriented. Preventing cyberbullying on university campuses requires dealing with risk factors related to the perpetrators, victims, the university environment, and the broader social culture. Males perpetrate cyberbullying at a higher rate than females, while females experience more victimization than males—a mutually significant relationship between cyberbullying victimization and cyberbullying perpetration. We should consider this relationship when establishing preventive measures.

Low self-control is a significant predictor of cyberbullying behavior. Students with high on low self-control are high on cyberbullying perpetration. Such students require training, educational, and psychological courses to improve self-control.

Findings showed a collective and unique significant effect of gender, college, father's work, exposure to violence, no interest in life, suicide ideation, anger, and low self-control on general cyberbullying. Slightly above thirty five percent (35.8%) of the sample reported cyberbullying outside the university campus. About half of the sample (45.3%) reported depression or hopelessness, lost interest in life or life enjoyment (45.3%), a willingness to die (32.8%), or suicide (30%). Cyberbullying can lead to mental health issues, increased stress, anxiety, depression, violent behavior, and low self-esteem, with long-lasting emotional effects even after the bullying has stopped. Cyberbullying can cause long-lasting emotional issues, including mood, energy, sleep, and appetite issues. Victims may experience self-doubt, worry, and lose inner peace. Cyberbullying can also tarnish a person's image and lead to enduring feelings of embarrassment and self-doubt (Gohal, Alqassim, Eltyeb, E. et al., 2023).

Significant differences are attributed to gender in general in relation to cyberbullying, cyberbullying victimization, cyberbullying perpetration, self-cyberbullying, vicarious cyberbullying, and low self-control. Studies show that in various educational settings, females are more likely to be involved in cyberbullying as victims than males. Cultural and sociological contexts influence this gender difference, with Asian countries, North America, and Europe exhibiting the most significant differences. These differences are attributed to dispositional and structural explanations. Boys socialize to be autonomous and goal-oriented, whereas girls' friendships are more intensive and intimate. Girls' socialization, positive self-focus on relationships, and empathetic connectedness suggest a greater interest in maintaining friendships and resolving conflict (Foody, McGuire, Kuldas, & O'Higgins, 2019).

There is a significant relationship between low self-control and violence victimization, violence participation, exposure to cyberbullying, knowledge of cyberbullying, knowledge of cyberbullying perpetration, self-cyberbullying, vicarious cyberbullying, and general cyberbullying. Additionally, there was a significant correlation between cyberbullying victimization, cyberbullying perpetration, self-cyberbullying, and vicarious cyberbullying. Youth cyberbullying behavior and overall cybercrime are associated with low self-control (LSC). Individuals with LSC are more likely to engage in cyberbullying than those with high self-control. Offline victimization and perpetration, or greater online time, mediate this association. (Sela-Shayovitz, Levy, & Hasson, 2024).

Cyberbullying Perpetration	Between groups	32.235	1	32.235	.370	.543
	Within groups	86926.901	998	87.101		
	Total	86959.136	999			
Self Cyberbullying	Between groups	226.850	1	226.850	1.961	.162
	Within groups	115464.869	998	115.696		
	Total	115691.719	999			
Vicarious Cyberbullying	Between groups	214.835	1	214.835	3.443	.064
	Within groups	62271.069	998	62.396		
	Total	62485.904	999			
Low Self-Control	Between groups	167.599	1	167.599	5.172	.023
	Within groups	32342.192	998	32.407		
	Total	32509.791	999			

4. Discussion

The results show that over a quarter (26%) participated in fights and experienced cyberbullying. There is a high prevalence of cyberbullying victimization and perpetration (73% and 76%, respectively), a widespread and prevailing cyberbullying behavior in the university environment. Cyberbullying has become a significant social and political issue in the world, sometimes leading to youth suicide. Governments are focusing on educational institutions to develop programs to combat cyberbullying in academic institutions. Factors such as anonymity, repetition, and a lack of structured environments complicate detection. Psychological support is crucial for students involved in cyberbullying attacks (Reyhani, 2015). The unique dynamics of social media may motivate or cause a significant number of children to engage in cyberbullying. Social media platforms promise privacy or anonymity; social media promotes sharing; communication through social media does not include face-to-face interaction; on social media, justice seems to mean bullying the bully; social media fosters a mob-like mentality, and we all crave likes, shares, and views (Organization for Social Media Safety, 2021).

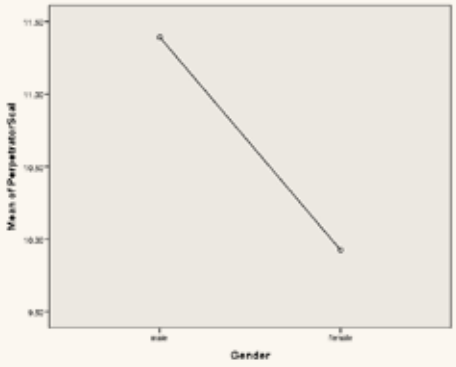


Figure 1 Gender mean differences in Cyberbullying Perpetration

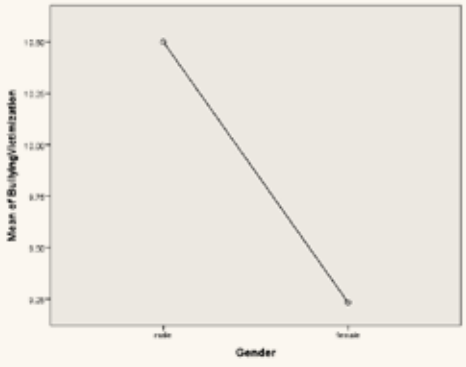


Figure 2 Gender mean differences in Cyberbullying Victimization

College Differences

Table 8 shows significant differences between science colleges and other colleges in some cyberbullying variables (general cyberbullying, vicarious cyberbullying, and low self-control). However, no significant differences were found between science colleges and other colleges in cyberbullying victimization, cyberbullying perpetrators, self-cyberbullying, and vicarious cyberbullying.

Table 8. College Differences in Cyberbullying variables and low self-control

	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
General Cyberbullying	Between groups	5570.172	1	5570.172	4.795	.029
	Within groups	1159411.732	998	1161.735		
	Total	1164981.904	999			
Cyberbullying Victimization	Between groups	2678.343	1	2678.343	2.300	.130
	Within groups	1162303.561	998	1164.633		
	Total	1164981.904	999			

Table 7. Gender differences in cyberbullying variables and low self-control

	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
General Cyberbullying	Between groups	5570.172	1	5570.172	4.795	.029
	Within groups	1159411.732	998	1161.735		
	Total	1164981.904	999			
Cyberbullying Victimization	Between groups	398.176	1	398.176	4.591	.032
	Within groups	86560.960	998	86.734		
	Total	86959.136	999			
Cyberbullying Perpetration	Between groups	533.586	1	533.586	4.624	.032
	Within groups	115158.133	998	115.389		
	Total	115691.719	999			
Self-Cyberbullying	Between groups	268.412	1	268.412	4.305	.038
	Within groups	62217.492	998	62.342		
	Total	62485.904	999			
Vicarious Cyberbullying	Between groups	124.023	1	124.023	3.822	.051
	Within groups	32385.768	998	32.451		
	Total	32509.791	999			
Low Self-Control	Between groups	371.599	1	371.599	7.823	.005
	Within groups	47402.832	998	47.498		
	Total	47774.431	999			

Table 5. Regression ANOVA table of all predictors on the cyberbullying perpetrator.

Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	17288.098	8	2161.012	21.763	.000
Residual	98403.621	991	99.297		
Total	115691.719	999			

Table 6. Unstandardized Coefficients and Standardized Coefficients on Cyberbullying Perpetrator.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	6.731	1.808		3.724	.000
LSC Scale	.434	.048	.279	9.093	.000
Gender	-1.188	.663	-.055	-1.791	.074
College	1.425	.667	.066	2.137	.033
Father Work	-1.672	.706	-.070	-2.367	.018
Child violence	-2.549	1.060	-.071	-2.404	.016
No Interest in Life	-3.907	.674	-.181	-5.798	.000
Suicide	2.415	.728	.103	3.316	.001
Anger	.998	.239	.127	4.186	.000

As can be seen from Table 6, each predictor (low self-control, anger, father's work, suicide ideation, gender exposure to violence in childhood, type of college, showing no interest in life) has a significant unique contribution to cyberbullying victimization.

Gender Differences

Table 7 shows a significant difference between males and females in all cyberbullying variables (general cyberbullying, cyberbullying victimization, cyberbullying perpetrator, self-cyberbullying, vicarious cyberbullying, and low self-control). Figures 1 and 2 show gender differences in cyberbullying victimization and cyberbullying perpetration.

Table 3. Regression ANOVA table of all predictors on cyberbullying victimization.

Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	9814.522	8	1226.815	15.760	.000
Residual	77144.614	991	77.845		
Total	86959.136	999			

Table 4. Unstandardized Coefficients and Standardized Coefficients on the cyberbullying victimization

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	7.632	1.601		4.768	.000
LSC Scale	.331	.042	.245	7.831	.000
Gender	-.997	.587	-.053	-1.697	.090
College	.762	.591	.041	1.291	.197
Father Work	-1.387	.625	-.067	-2.218	.027
Child violence	-2.687	.939	-.086	-2.862	.004
No Interest in Life	-1.939	.597	-.103	-3.250	.001
Suicide	2.419	.645	.119	3.750	.000
Anger	.736	.211	.108	3.485	.001

As can be seen from Table 4, each predictor (low self-control, anger, father's work, suicide ideation, exposure to violence in childhood, type of college, showing no interest in life) has a significant unique contribution (exceptgender) on cyberbullying victimization.

Factors affecting cyberbullying perpetration

As can be seen from Table 5, regressing low self-control, anger, father's work, suicide ideation, gender, exposure to violence in childhood, type of college, and showing no interest in life on cyberbullying victimization showed a significant effect of all these variables (F = 15.760, α =.000). However, all predictors explained 16% of the variance on cyberbullying perpetration.

Table 1. Regression ANOVA table of all predictors on the General cyberbullying.

Source	Sum of squares	df	Mean square	F	Sig.
Regression	174249.850	8	21781.231	21.787	.000
Residual	990732.054	991	999.730		
Total	1164981.904	999			

Table 2. Unstandardized Coefficients and Standardized Coefficients on cyberbullying generally.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	23.072	5.736		4.023	.000
Low self-control	1.360	.151	.275	8.979	.000
Gender	-4.031	2.105	-.059	-1.915	.056
College	4.875	2.116	.071	2.304	.021
Father Work	-6.272	2.241	-.083	-2.799	.005
Exposure to violence	-9.165	3.365	-.080	-2.724	.007
No Interest in Life	-10.690	2.138	-.156	-5.000	.000
Suicide	8.480	2.311	.114	3.669	.000
Anger	3.286	.757	.132	4.342	.000

Table 2 shows that each predictor—low self-control, anger, father's work, suicide ideation, gender, exposure to childhood violence, type of college, and showing no interest in life—contributes significantly and uniquely to cyberbullying.

Factors affecting cyberbullying victimization

As can be seen from Table 1, regressing low self-control, anger, father's work, suicide ideation, gender, exposure to violence in childhood, type of college, and showing no interest in life on cyberbullying victimization showed a significant effect of all these variables ($F = 15.760$, $\alpha = .000$). However, all predictors explained 16% of the variance in cyberbullying victimization.

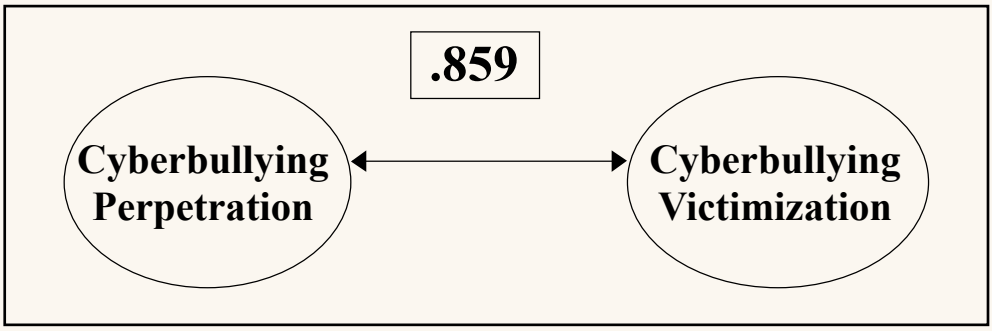
Table: The relationship between Cyberbullying victimization, Cyberbullying perpetration, self-reported Cyberbullying, and vicarious cyberbullying

	Cyberbullying victimization	Cyberbullying perpetration	Self Report cyberbullying	Vicarious cyberbullying
Cyberbullying victimization	**1**	.859	.807	.810
Cyberbullying Perpetration	.859	**1**	.943	.911
Self report-Cyberbullying	.807	.943	**1**	.950
Vicarious cyberbullying	.810	.911	.950	**1**

**. Correlation is significant at the 0.01 level (2-tailed).

The Relationship Between Cyberbullying Victimization and College Students' Cyberbullying Perpetration

The study found that cyberbullying victimization positively predicts cyberbullying perpetration in college students. This is consistent with previous research, as negative emotions, such as anger, can trigger cyberbullying. The anonymity of the network environment increases the likelihood of victims venting their negative feelings, leading to increased cyberbullying perpetration (Dou, Xiang, Sun, & Chen, 2020; Özdemir, Kuzucu, 2015; Linton, & Power, 2012; Law, Shapka, Hymel, & Olson, 2011).



Factors Affecting General Cyberbullying

As can be seen from Table 1, regressing low self-control, anger, father's work, suicide ideation, gender, exposure to violence in childhood, type of college, and showing no interest in life on general cyberbullying showed a significant effect of all these variables (F = 21.787, α =.000). However, in general, all predictors explained 15% of the variance on cyberbullying.

	1	2	3	4	5	6	7	8	9
1. Low Self-Control	**1**								
2. Exposure to Violence	.013	**1**							
3. Violence Victims	.149**	.008	**1**						
4. Participation in Violence	.170**	.023	.17**	**1**					
5. Exposure to Cyberbullying	.132**	.032	.10**	.173**	**1**				
6. Knowledge Cyberbullying Victims*	-.13**	-.013	-.16**	-.21**	-.20**	**1**			
7. Knowledge Cyberbullying Perpetrator*	-.14**	-.03	-.17**	-.18**	-.22**	.489**	**1**		
8. Self-report Cyberbullying	.276**	-.08*	.018	.052	.069*	.094**	.059	**1**	
9. Vicarious Cyberbullying	.279**	-.08*	.011	.053	.076*	.087*	.052	.950**	**1**
10. General Cyberbullying	.289**	-.09*	.033	.050	.062	.080*	.056	.962**	.949**

**Correlation is significant at the 0.01 level (2-tailed).* coding know 1= yes do not know =0

*Correlation is significant at the 0.05 level (2-tailed).

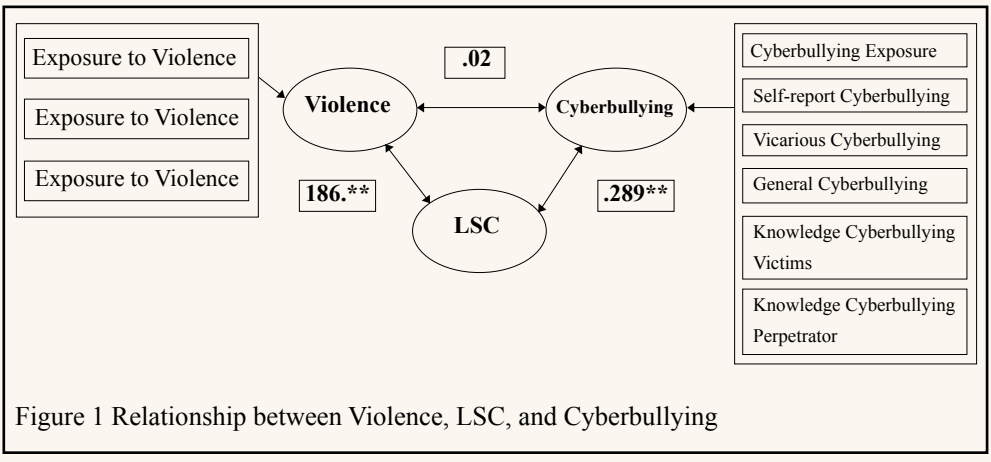


Figure 1 Relationship between Violence, LSC, and Cyberbullying

Violence Measures

I. **Exposure to family violence.** The dichotomy level by asking a general family violence question: In the last 12 months, have you been exposed to family violence? Responses were (1—yes, 0—no).
II. **Exposure to any violence.** The dichotomy level by asking a general violence question: In the last 12 months, have you been exposed to family violence? Responses were (1—yes, 0—no).
III. **Participation in Violence.** The dichotomy level by asking a general family violence question: In the last 12 months, have you been participating in any violence? Responses were (1—yes, 0—no).

Procedure

Trained researchers distributed the survey to all participants. They explained the study's purpose, confidentiality, and instructions for completing the survey. The researchers obtained informed consent from all students and requested their voluntary participation, allowing them to withdraw from the study whenever they wished.

3. Findings

The results show that 26% of the sample participated in fights and experienced cyberbullying. Less than 10% of the sample (9.3%) reported knowledge about cyberbullying, and 35.8% reported it outside the university campus. Moreover, more than 10 percent of the sample (13.5%) reported knowledge about cyberbullying perpetrators, and 33% reported it outside the university campus. About half of the sample (45.3%) reported depression or hopelessness, lost interest in life or life enjoyment (45.3%), a willingness to die (32.8%), or suicide (30%).

The Relationship Between Exposure to Violence, Cyberbullying, and Low Self-Control

Table 1 shows a significant relationship between low self-control, all violence variables, and cyberbullying variables, except exposure to violence.

Table 1: Correlation coefficients between exposure to family violence, violence victimization, participation in violence, low self-control, and cyberbullying among college students

were females. The sample comprised 496 students (49.6%) from science colleges and 504 students (50.4%) from other colleges. Around a quarter of the sample (26%) were exposed to cyberbullying, 9% knew victims of cyberbullying on the university campus, and 36% knew victims outside the campus. Around a quarter (26%) of the sample participated in violence.

2.2 Measurement

The **victimization of cyberbullying** is measured at different levels:

1. **General cyberbullying scale**. This scale is based on the literature review. It consists of 34 items covering cyberbullying victimization, self-reported victimization, and perpetration. Questions are on interval levels 0-5 (0 no to 5 most frequently). The scale's Cronbach's α was 0.99, and the validity (correlation between the scale and LSC scale) was 0.29 α=0.00.

2. **Cyberbullying subscales**

   A. **Exposure to Cyberbullying.** One single-item scale. In the last 12 months, were you exposed to cyberbullying? Responses were (1—yes, 0—no).
   B. **Knowledge of cyberbullying victims**: one single-item scale. In the last 12 months, did you know victims of cyberbullying? Responses were (1—yes, 0—no).
   C. **Knowledge of cyberbullying perpetrators**. This was a one-item scale. In the last 12 months, did you know the perpetrators of cyberbullying? Responses were (1—yes, 0—no).
   D. **Cyberbullying victimization Scale.** This scale is based on the Revised Olweus Bully/Victim Questionnaire. It consists of 10 items for victims on interval levels 0-5 (0 no to 5 most frequently). The scale's Cronbach's α was 0.95, and the validity (correlation between the scale and Low Self Control (LSC) scale) was 0.26 α=0.00.
   E. **Cyberbullying perpetration scale**. This scale is based on the Revised Olweus Bully/Victim Questionnaire. It consists of 10 items for perpetrators on interval levels 0-5 (0 no to 5 most frequently). The scale's Cronbach's α was 0.97, and the validity (correlation between the scale and LSC scale) was 0.29 α=0.00.
   F. **Self-report cyberbullying scale.** It consists of 5 items: cyberbullying using text, emails, pictures, videos, and blackmailing. The scale's Cronbach's α was 0.97, and the validity (correlation between the scale and LSC scale) was 0.28 α=0.00.
   G. **Vicarious cyberbullying scale.** It consists of 5 items: cyberbullying using text, emails, pictures, videos, and blackmailing. The scale's Cronbach's α was 0.96, and the validity (correlation between the scale and LSC scale) was 0.28 α=0.00.

10th of the sample (9.3%) knew about cyberbullying, 9% were aware of victims on the university campus, 35.8% reported its existence off-campus, and 13.5% reported knowing cyberbullying perpetrators. About a third of the sample (30%) reported experiencing cyberbullicide ideation (12.9% males and 17.1% females), with a high level of cyberbullicide ideation found among victims of violence (16%) and cyberbullying (8.7%). Almost half of the sample (45.3%) reported depression or hopelessness, no interest in life or life enjoyment (45.3%), willingness to die (32.8%), or cyberbullicide ideation (30%). A fifth of participating students reported bullying victimization, and a 10th reported cyberbullying. Results showed that cyberbullying variables could explain a 100% change in cyberbullicide ideation. The logistic regression model correctly classified 70.9% of the cases' overall predictions. Furthermore, students of Arts colleges (18%) experienced cyberbullicide ideation more than students of Sciences colleges (12%). The study supported the hypothesis that students' cyberbullying victimization could lead to cyberbullicide and in the least serious scenario to cyberbullicide ideation (Al-Badayneh, Khelifa & Ben Brik, 2024).

A study examines workplace cyberbullying among academic staff at Jordanian universities, revealing that it reduces with increasing social capital. However, no relationship was found between cyberbullying and self-esteem. A positive correlation was found between self-esteem and structural social capital. The findings suggest that Jordanian administrators and policymakers should improve social capital among academics to prevent distress and improve organizational life (Alrawashdeh, Alsawalqa, Alnajdawi, et al., 2024).

Al-badayneh et al., (2023), investigates the social determinants and strains of cyberbullying victimization among expatriate populations in high-income countries like Qatar. The investigation suggests that factors like alienation, loneliness, homesickness, insecurity, and helplessness contribute to victimization. The study found that 10.8% of expats reported cyberbullying, with 24% being males and 5.8% females. Victims were mostly from intact families, with a third reporting the absence of a father during childhood. Most victims did not use seat belts and avoided gambling (Al-badayneh, ben Brik, & Elwakad, 2023).

2. Methodology

2.1 Sample.

The study sample comprised 1000 Jordanian students representing 12 Jordanian governorates. The sample was selected randomly from different colleges and levels. Of these students, 454 (45.4%) were males, and 546 (54.6%)

Over 1 million children in Amman, Jordan, participated in the national campaign "The New Epidemic at The Time of The Pandemic" by the National Council for Family Affairs and UNICEF Jordan to combat cyberbullying. The campaign, launched in 2017 as part of the National Plan for ending violence against children, aimed to raise public awareness about cyberbullying and internet safety. The campaign engaged 60 online activists and influencers on social media platforms, promoting knowledge on safe internet usage and digital protection policies. The campaign attracted 57% of young followers, mainly from Amman. The campaign aimed to stimulate positive interaction with young people and raise awareness at the national, institutional, academic, and grass-roots level, requiring necessary interventions, policies, legal support, and psychosocial support to deal with victims of cyberbullying. (National Council for Family Affairs, 2021).

A study by Al-badayneh et al. (2024b) investigates the link between cyberbullying and depression among college students. It involved 1,000 Jordanian students from Tafila Technical University, representing 12 governorates. Results showed that 26% of students experienced violence and 9% knew cyberbullying victims. 37% reported depression, 33% had a death wish, and 45% had no interest in life. Cyberbullying significantly correlated with depression and low self-control, with factors such as fear, anger, gender, college type, and father's work status explaining 86% of the depression variable (Al-Badayneh, Khelifa, & Aladra, 2024). Another study examines strain variables affecting cyberbullying victimization among college students in Qatar. Results show a 49% change in victimization, with significant gender and mean differences between bullied and non-bullied students. The findings support the General Strain Theory's hypothesis that cyberbullying victimization can lead to delinquency (Al-badayneh, Al-Hafry, & Ben Brik, 2022).

A study found that 30.1% of Jordanian nursing students were not involved in cyberbullying, while 8.6% were perpetrators and 20.4% victims. Visual/sexual and verbal/written victimization were prevalent. Age and male gender were associated with decreased cyberbullying. The study revealed alarming cyberbullying prevalence among nursing students, with age as a factor negatively affecting CBP and CBV, and being male increasing CBP. Future research should use longitudinal design and develop specific policies (Al-Shatnawi, Ababneh, Elemary, Rayan & Baqeas, 2024).Al-Badayneh et al. (2024A) investigated the impact of cyberbullying on youth cyberbullicide ideation (i.e., cyberbullying victimization, cyberbullying perpetrator, and low self-control). Findings revealed that students experienced cyberbullying. Approximately 26% of the sample experienced cyberbullying in general, 73% knew cyberbullying victims, and 64% knew cyberbullying perpetrators. Nearly a

studied attack. It manifests itself as visual and written-verbal behaviors, with visual behaviors being more severe. Cyberbullying is most prevalent among early teens but can begin in middle school and continue into college.

Relevant literature Review

Victims often vent their emotions through cyberbullying and become perpetrators themselves, contributing to a vicious cycle. Cyberbullying is characterized by anonymity, spatial spread, and robust propagation, affecting victims' physical and psychological health (Dou, Xiang, Sun, & Chen, 2020).

For a perpetrator, the path to a cyberbullying encounter starts with personal and situational factors that affect the individual's internal state. This can lead to hostile thoughts, negative effect, and heightened arousal. Depending on the situation, the victim's response can be impulsive or more thoughtful. Over time, these encounters can lead to distal outcomes, such as decreased popularity or school performance, affecting individual and situational factors. For example, a young boy may become a cybervictim after receiving a message, putting him in a state of distress. The victim's response can feed back into previous maladaptive behavior and provocation, potentially affecting future encounters (Kowalski et al., 2009).

Early life experiences shape low self-control, as Gottfredson and Hirschi (1990) identified. It includes six dimensions: impulsivity, insensitivity, preference for physical activity, risk-taking tendency, shortsightedness, and nonverbal orientation. Individuals with low self-control tend to prefer immediate gratification, have lower verbal abilities, and struggle with concentration. There is a belief that criminal behavior and imprudent behaviors such as drinking, smoking, and gambling are associated with low self-control (Gottfredson & Hirschi, 1990; Grasmick, Tittle, Bursik, & Arneklev, 1993; Hay, & Forrest, 2008). The general strain theory (GST) suggests that cyberbullying victimization, as a negative stimulus, can lead to cyberbullying perpetration. Studies have found a significant correlation between victimization and cyberbullying perpetration, suggesting that victims are likely to become perpetrators. Anger, a coping strategy, can also middle in this relationship. Stress and strain can trigger negative emotions like anger, which in turn increases the likelihood of engaging in cyberbullying. According to various studies (Kraft & Wang, 2011; Patchin & Hinduja, 2011; Mcgrath, 2017), being bullied online can increase the likelihood of engaging in cyberbullying.

while others are more specific regarding technology taxonomy. Cyberbullying can take various forms and occur through various venues, including flaming, harassment, outings and trickery, exclusion, impersonation, cyberstalking, and sexting (Kowalski et al., 2009). According to Werner et al. (2010), using the internet to threaten or embarrass someone, such as posting or sending messages about them for others to see, or instructing others to block instant messages from someone you dislike or are angry with, using the internet to play a joke or annoy someone you're angry at, or making rude or nasty comments about someone else online (Werner et al. 2010, p. 330) are examples of such behavior. Willard (2005) categorizes cyberbullying into seven forms: flaming, harassment, denigration, impersonation, outing and trickery, exclusion, and cyberstalking, involving harmful or cruel texts or images (Willard, 2005). Various factors influence cyberbullying behavior in adolescents, including personality traits, traditional cyberbullying, perception of the victim, strain, and parental interaction. Other internal factors, such as self-control, also play a role. Factors influencing cyberbullying include individuals, families, friends, schools, and social media use (Kowalski et al., 2009).

Cyberbullying in university colleges leads to negative consequences for both victims and perpetrators. Victims may experience physical, psychological, and academic problems, while bullies are more likely to commit criminal behaviors as young adults. Recent research suggests that low self-control theory, which suggests youths with low self-control, empathy, and impulsivity are more likely to engage in cyberbullying, may explain the etiology of school cyberbullying. We need more research to better understand this issue (Moon & Alarid, 2015).

Cyberbullying, which occurs through electronic media and is widespread, affects cybervictims. The average annual cybervictimization rate is 14–21%, with 10–72% of youths globally reporting being victims. Cybervictims often experience mental health problems, stress, and maladaptive regulation strategies that lead to suicide. Cybervictimization is a strong predictor of cyberbullying, with some cybervictims responding with cyberbullying behavior. Cyberbullying victims frequently commit it in the same online environment where they experienced it. Previous cybervictimization experiences positively predict subsequent cyberbullying behavior, and some argue that cybervictims would perpetrate cyberbullying. The vicious cycle of cybervictimization and cyberbullying is a significant concern (Luo, Wu N., Huang, 2023).

A group or individual using electronic contact can carry out an aggressive, intentional act known as cyberbullying, which has become a familiar and widely

by the influence of family and online environments, which can trigger aggressive behaviors. Cyberbullying, primarily verbal and relational cyberbullying, has become more prevalent among adolescents, causing severe and long-lasting psychological trauma. This study aimes to understand the influencing factors of cyberbullying behavior to prevent and reduce such deviant behaviors and enhance students' psychological health. The study is unique regarding geographic heterogeneity, scientific selection, and the use of integrated combinations of variables. Violence exposure, which includes witnessing and experiencing domestic violence firsthand, is a significant factor in adolescent aggressive behavior. Adolescents who witness or experience domestic violence tend to view violence as an acceptable approach to resolving interpersonal conflicts and internalize it as a stable personality trait, increasing the likelihood of engaging in cyberbullying behaviors in the future. Exposure to domestic violence has a significant impact on adolescents' emotional and behavioral problems, with inter-parental violence being more important than other forms of destructive conflict. According to a study by Chen et al. (2023), exposure to domestic violence has a positive impact on cyberbullying among secondary school students, with depression partially mediating the relationship and self-control alleviating the effects while intensifying depression's effect (Chen et al., 2023).

Cyberbullying is a widespread issue among children and adolescents, causing emotional, social, and psychiatric problems that can persist into adulthood. Research on cyberbullying is limited, but it provides insight into the psychosocial and academic consequences of cyberbullying. Students who are cyberbullied report feelings of sadness, anxiety, and fear, which affect their grades. They are also more likely to skip school, have detentions or suspensions, or bring a weapon to school. Research shows that depression, substance use, and delinquency are significantly higher among youth who report experiencing cyberbullying or online sexual solicitation. Furthermore, perpetrators of cyberbullying are more likely to break the rules and act aggressively. We need a survey with a diverse sample of middle school and college students to understand its prevalence and impact better, as the literature on cyberbullying is limited (Mishna et al., 2010).

Defining Cyberbullying

Cyberbullying is the use of electronic communication technologies to bully others, but defining its prevalence remains challenging due to a lack of consensus on specific parameters. Standard operational definitions vary in specificity versus generality, with some defining it as cyberbullying via the internet or mobile phones,

Southern and Eastern Asia and Africa. However, more work is needed to achieve universal access. Despite mobile phones being the primary mode of internet use, over 6 in 10 users still use laptops and desktops for online activities (Kepios, 2024). In early 2023, Jordan had 9.95 million internet users, with internet penetration at 88.0%. The country had 6.61 million social media users, accounting for 58.4% of the total population. There were 8.61 million cellular mobile connections, equivalent to 76.1% of the population. Internet usage increased by 6.8% between 2022 and 2023. However, 1.36 million people in Jordan did not use the internet, indicating that 12.0% of the population remained offline. The median mobile internet connection speed in Jordan decreased by 2.76 Mbps (-14.3 percent) in the twelve months to the start of 2023, while fixed internet connection speeds increased by 21.10 Mbps (+39.5%). The latest published figures for internet use may under-represent reality, and actual adoption and growth may be higher than the figures suggest (Simon Kemp, 2023). Internet freedom in Jordan is limited, with government surveillance and restrictions on online activity. WhatsApp gets suspended during high school exams in an attempt to prevent cheating and TikTok is blocked, and journalists can face prosecution for criticism. The government also issues gag orders to limit media coverage of politically sensitive topics. In August 2023, the king approved a new Cybercrime Law, imposing criminal penalties for online speech and circumvention tools. The monarchy's electoral system disadvantages opposition, and the judicial system lacks independence and due process (Freedom on the Net, 2023). A report by the Market Research Unit of the Information and Communications Technology Association of Jordan (Intaj) shows that 91% of Jordanians are connected to the internet. 77% prefer mobile devices for internet access, while only 22% use laptops. Google Chrome is the preferred browser, with Android users accounting for 79%. Social media accounts account for 56% of the Jordanian population. LinkedIn is the most popular platform among women, with 33% using it. Snapchat is also popular, with 54% using it. Instagram is also popular, with 50% of female users using it (The Jordan Times, 2024).

Bullying, including cyberbullying, involves power imbalances and harmful messages sent via digital technologies. It poses significant health risks to teenagers worldwide, often linked to off class bullying. Cyberbullying provides anonymity, increasing danger to minors. If linked to suicide, legal proceedings may be initiated (Schonfeld et al., 2023, Daniela & Felicia, 2022). Victims may experience depression, anxiety, social frustration, and emotional pressure (Kamath et al., 2021).

Cyberbullying, a hidden, repetitive issue, can significantly impact secondary school students' physical and mental health due to its indirect nature, exacerbated

1. Background

The widespread use of technology among young people has led to cyberbullying, causing harmful discourse and a surge in cyberbullicide ideation (Schonfeld et al., 2023). College students are both perpetrators and victims, with severe mental health consequences (Maurya et al., 2022; Kumar et al. (2021). The internet has revolutionized education, making it more accessible. However, it has also led to a rise in cyberbullying, a phenomenon linked to high-profile adolescent suicides, highlighting the need for a comprehensive understanding of this issue (Mitsu, & Dawood, 2022).

Bullying is aggressive behavior that repeatedly causes injury or discomfort, often through physical contact or words. Cyberbullying, on the other hand, involves using technology to harass, hurt, embarrass, humiliate, or intimidate another person, often through text, apps, or online platforms. Cyberbullying can sometimes escalate into unlawful or criminal behavior (Hinduja, & Patchin, 2019).

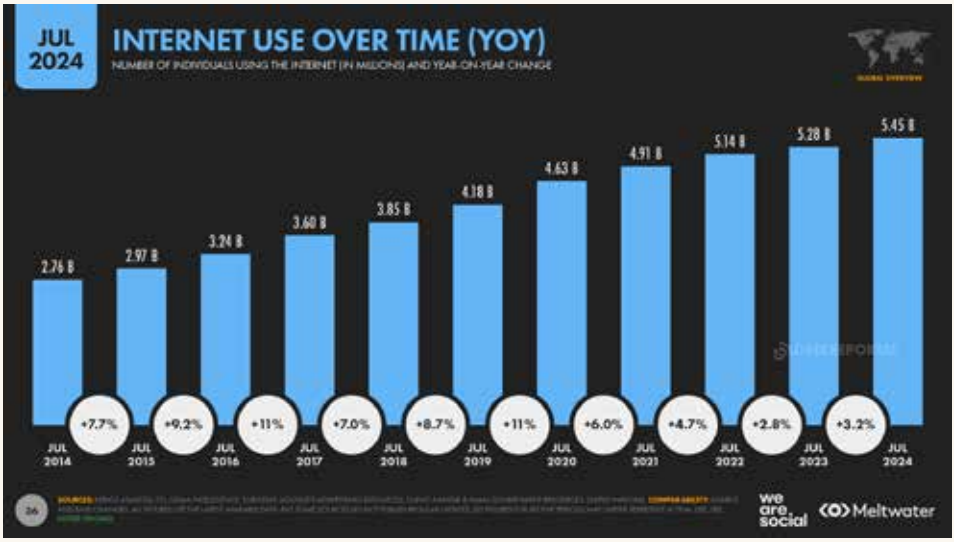


Figure 1 Internet uses 2014-2024

As of July 2024, 5.45 billion people worldwide have become internet users, making them a "supermajority". The connected population grew by 167 million users in 12 months up to July 2024, a 3.2% year-on-year growth rate. However, delays in research of internet adoption may suggest a higher real growth rate. Global internet access has reduced the number of unconnected people to 2.67 billion, primarily in

المُلخَّص

العوامل المؤثرة على التنمر السيبراني، وضحايا التنمر السيبراني، وارتكاب التنمر السيبراني بين طلاب الجامعات

الأستاذ الدكتور /ذياب البداينة
أستاذ علم المنهجية وعلم الجريمة وعلم النفس الجنائي - عضو هيئة التدريس بكلية الدراسات العليا - أكاديمية الشرطة - دولة قطر

تبحث هذه الدراسة في العوامل المؤثرة في التنمر السيبراني بشكل عام، والوقوع ضحية للتنمر السيبراني، وارتكاب التنمر السيبراني بين طلاب الجامعات في الأردن. شمل المسح الاجتماعي عينة مكونة من 1000 طالب أردني تم اختيارهم عشوائيًا من 12 محافظة. تبين أن 26 % من العينة تعرضوا للتنمر السيبراني، وأن 73 % كانوا على دراية بالوقوع ضحية للتنمر السيبراني، وأن 80 % كانوا على دراية بارتكاب التنمر السيبراني، وأن 9 % كانوا على دراية بالضحايا داخل الحرم الجامعي وخارجه.

تظهر النتائج أن النوع الاجتماعي، والكلية، وعمل الأب، والتعرض للعنف، وعدم الاهتمام بالحياة، وأفكار الانتحار، والغضب، وانخفاض ضبط الذات تؤثر بشكل كبير على التنمر السيبراني بشكل عام، والوقوع ضحية للتنمر السيبراني، وارتكاب التنمر السيبراني. كما تبين الدراسة وجود فروق ذات دلالة إحصائية تعزى للنوع الاجتماعي في التنمر السيبراني، والوقوع ضحية للتنمر السيبراني، والتنمر السيبراني الذاتي، والتنمر السيبراني غير المباشر، وانخفاض ضبط النفس. تمت مناقشة التدابير الوقائية في التعليم العالي.

الكلمات المفتاحية: التعرض للتنمر السيبراني، التنمر السيبراني، ضحايا التنمر السيبراني، ارتكاب التنمر السيبراني، طلاب الجامعات، الأردن.

Factors Affecting Cyberbullying, Cyberbullying Victimization, and Cyberbullying Perpetration Among College Students

Professor Dr. Dhiab Al-Badayneh
Professor of Methodology, Criminology and Forensic Psychology
Faculty member at the graduate studies department at Police Academy, Qatar

ABSTRACT

The study investigates factors affecting cyberbullying, cyberbullying victimization, and cyberbullying perpetration among college students in Jordan. A survey of 1000 randomly selected Jordanian students from 12 governorates revealed that 26% had experienced cyberbullying, 73% were aware of cyberbullying victimization, 80% were aware of cyberbullying perpetration, and 9% were aware of victims both on and off campus.

Results show that gender, college, father's work, exposure to violence, no interest in life, suicidal thoughts, anger, and low self-control significantly affect cyberbullying, victimization, and perpetration. Gender, as a factor, also has significant differences in cyberbullying, victimization, perpetration, self-cyberbullying, vicarious cyberbullying, and low self-control. Preventive measures are discussed in higher education.

Keywords: Exposure to cyberbullying, cyberbullying, cyberbullying victimization, cyberbullying perpetration, college students Jordan.

Factors Affecting Cyberbullying, Cyberbullying Victimization, and Cyberbullying Perpetration Among College Students

Professor Dr. Dhiab Al-Badayneh

Professor of Methodology, Criminology and Forensic Psychology

Faculty member at the graduate studies department at Police Academy, Qatar

Researches & Studies In English

8) le processus d'examen des recherches et études soumises pour publication dans la revue est une étape majeure de la publication scientifique, et donc les members du comité de lecture - internes et externes - doivent adhérer à l'éthique de la publication scientifique et à ses principes.

9) la revue suit l'approche de l'arbitrage caché (aveugle) de sorte que l'arbitre ne connaît pas l'identité du chercheur, tout comme le chercheur ne connaît pas l'identité de l'arbitre.

10) la recherche est soumise à un programme de filtrage des citations avant de l'envoyer pour examen, et en cas de dépassement de 25% d'une référence, ou de 25% des références dans leur ensemble, la recherche est renvoyée à l'auteur.

11) l'arbitre doit se distancier de ses intérêts personnels, par exemple en utilisant les informations obtenues à partir de la recherche qui a été arbitrée pour son bénéfice personnel.

12) l'arbitre doit en informer le rédacteur en chef ou le directeur de la rédaction, au cas où il n'accepterait pas ou ne serait pas prêt à arbitrer la recherche ou l'étude, dès réception, afin que la recherche ou l'étude puisse être envoyée à un autre arbitre dans le délai imparti.

13) l'arbitre doit se conformer aux normes de confidentialité relatives au processus d'examen et traiter les recherches et études soumises à l'examen comme des documents confidentiels, qui ne peuvent être divulgués pendant la phase d'examen, ni discutés avec d'autres personnes que le rédacteur en chef ou le directeur éditorial.

14) l'arbitre exprimera son opinion scientifique dans les recherches et études qui lui sont envoyées aux fins de l'arbitrage avec intégrité, objectivité et clarté, avec l'inclusion dans le rapport d'examen des arguments étayant ce qu'il conclut sur la validité de la recherche ou de l'étude pour publication ou non.

15) l'arbitre -interne et externe- doit respecter le temps alloué au processus d'examen.

II - Ethique de la publication:

La revue adopte les normes d'éthique de la recherche et de la publication scientifique, et à la lumière de ces normes:

1) la recherche soumise pour publication ne doit pas avoir été préalablement publiée par quelque moyen de publication que ce soit, et elle ne doit être soumise à aucun autre organisme d'édition pendant la période de son examen, et le chercheur s'engage à le faire par écrit.

2) la recherche ou l'étude ne doit pas faire partie d'une thèse de master ou d'une thèse de doctorat préalablement préparée par le chercheur, ni d'un ouvrage précédemment publié, ni de tout autre ouvrage publié pour préserver les droits de propriété intellectuelle.

3) adhérer aux règles de la recherche scientifique et à ses principes en termes de méthodologie de division, les règles de la documentation des références, l'integrité scientifique, et que la recherche doit inclure une conclusion qui comprend le résumé de la recherche, ses résultats et les recommandations proposées, et être accompagné d'une liste de références invoquées par le chercheur.

4) soumettre une recherche pour publication dans la revue est un consentement implicite pour permettre à la revue de rendre la recherche disponible sous n'importe quelle forme et dans n'importe quelle base de données ou référentiel numérique sans référence au chercheur.

5) si une recherche ou une étude est réalisée par plusieurs chercheurs, la portée et la nature des contributions individuelles de chacun d'eux doivent être déterminées. Chaque chercheur qui établit son nom sur la recherche ou l'étude doit avoir une contribution intellectuelle significative à la recherche ou à l'étude. Le simple financement ou la compilation de données ne sont pas des critères suffisants pour établir le droit d'auteur d'une personne.

6) tout conflit d'intérêts potentiel entre la personnalité du chercheur et tout organisme scientifique ou de recherche auquel le chercheur appartient, ou ayant un droit accessoire à la recherche ou à l'étude, doit être divulgué. Toute relation personnelle ou financière entre le chercheur et toute personne ou organisation susceptible d'affecter l'interprétation par le chercheur des résultats de sa recherche ou de son étude doit également être divulguée. Ceci doit être documenté par écrit lors de la soumission de la recherche ou de l'étude pour publication dans la revue.

7) le chercheur doit mentionner toutes les sources de financement de la recherche ou de l'étude. S'il existe une source de financement, le chercheur doit indiquer - en détail - le nom de l'organisme de financement ou du donateur.

I- Conditions de publication dans la revue:

La revue accueille favorablement la publication de recherches et d'études en Arabe, Anglais et Français selon les conditions suivantes:

1) la recherche soumise pour publication ne doit pas avoir été préalablement publiée par quelque moyen de publication que ce soit, et elle ne doit être soumise à aucun autre organisme d'édition pendant la période de son examen, et le chercheur s'engage à le faire par écrit.

2) la recherche doit être caractérisée par la modernité, la méthodologie scientifique, avec l'intégrité de la langue, et la comparaison avec la loi Qatarie autant que possible.

3) le nombre de pages de la recherche ou de l'étude ne doit pas dépasser (40) pages. Toutefois, le comité de rédaction de la revue peut, à titre exceptionnel, déroger à cette exigence si la nature du sujet de recherche ou d'étude l'exige.

4) le chercheur doit envoyer son curriculum vitae récent, y compris ses diplômes scientifiques.

5) la priorité de publication des recherches et études juridiques et de sécurité acceptées pour publication sera fonction de la priorité de réception des rapports des arbitres avec leur validité pour publication.

6) le Comité de Rédaction exclut toute recherche ou étude contraire aux règles de publication dans la revue ou aux exigences d'intérêt public.

7) l'ordre des recherches et des études acceptées pour publication dans les numéros de la revue est soumis aux considérations de pertinence appréciées par le comité de rédaction.

8) les recherches et études publiées dans la revue expriment les opinions de leurs auteurs et ne représentent pas l'opinion de la Revue, et l'auteur de la recherche ou de l'étude en porte la responsabilité légale.

9) les articles ou études envoyés à la Revue ne sont pas retournés à leurs propriétaires, qu'ils soient acceptés ou non pour publication dans la revue.

9) The Journal follows the approach of hidden (blind) arbitration so that the arbitrator does not know the personality of the author, just as the latter does not know the personality of the arbitrator.

10) The research is subjected to a citation screening program before sending it for review, and in case of exceeding 25% of one reference, or 25% of the references as a whole, the research is returned to the author.

11) The arbitrator shall distance himself from personal interests, such as using information obtained from the research that was arbitrated for his personal benefit.

12) The arbitrator must notify the editor-in-chief or the editorial director, in case he does not accept or is not ready to arbitrate the research or study, immediately upon receipt, so that the research or study can be sent to another arbitrator within the specified time frame.

13) The arbitrator must comply with the confidentiality standards related to the arbitration process, and treat the research and studies subject to arbitration as confidential documents, which may not be disclosed during the arbitration stage, or discussed with others except the editor-in-chief or editorial director.

14) The arbitrator shall express his scientific opinion in the researches and studies sent to him for the purposes of arbitration with integrity, objectivity and clarity, with the inclusion in the arbitration report of the arguments supporting what he concludes about the validity of the research or study for publication or not. 15) The arbitrator - internal and external - must comply with the time allocated for the arbitration process.

15) The arbitrator - internal and external - must comply with the time allocated for the arbitration process.

II- Publishing ethics

The Journal adopts the standards of research ethics and scientific publishing, and in light of these standards:

1) the work submitted for publication should not have been previously published by any means of publication, and it should not be submitted to any other publishing body during the period of its evaluation, and the researcher undertakes to do so in writing.

2) the work shall not be part of a Master's or PhD thesis previously prepared by the author, or part of a previously published book, to preserve intellectual property rights.

3) The author shall adhere to the rules and principles of scientific research in terms of segmentation methodology, referencing rules and scientific integrity. The work shall include a conclusion including a summary as well as the outcomes and recommendations. It shall also include the list of references used by the author.

4) Submitting a work for publication in the Journal is an implicit consent to allow the Journal to make it available in any form and in any database or digital media without reference to the author.

5) In case of multiple authors of one work, the scope and nature of the individual contributions of each of them should be determined. Every co-author who mentions his name on the work must have a significant intellectual contribution to this work. Mere funding, or the compilation of data, are not sufficient criteria to establish a person's right to authorship.

6) Any potential conflict of interest between the author's personality and any scientific or research body to which he may belong, or having an ancillary right to research or study, must be disclosed. Any personal or financial relationship between the author and any person or organization that may affect the author's interpretation of the results of his/her work should also be disclosed. This shall be documented in writing when submitting the work for publication in the Journal.

7) The author shall mention all funding sources of the work. If there is a source of funding, the author must indicate - in detail - the name of the funding agency or donor.

8) The process of evaluation of the work submitted for publication in the Journal is a major stage of scientific publishing, and therefore the arbitrators - internal and external - must adhere to the ethics of scientific publishing and its principles.

I- Conditions of publication in the journal:

The Journal welcomes the submission of research and studies in Arabic, English and French according to the following rules and regulations:

1) The author pledges that the submitted work has never been published in any other means of publication, and undertakes not to submit it to any other party during the period of its evaluation.

2) The work shall be characterized by modernity and scientific methodology required by scientific research, in addition to sound language and comparison with Qatari law when possible.

3) The number of pages of research or study should not exceed (40) pages. However, the editorial board of the journal may exceptionally override this requirement if the nature of the subject of research or study requires it.

4) The author should send his / her recent resume, including his/her scientific degree.

5) The priority in publishing of legal and security researches and studies accepted for publication shall be according to the priority of receipt of the arbitrators ' reports with their validity for publication.

6) The Editorial Board shall exclude any research or study, which are not compliant with the rules of publication in the journal, or the requirements of public interest.

7) The order of research and studies accepted for publication in the issues of the Journal is subject to the considerations of appropriateness appreciated by the Editorial Board.

8) The works published in the Journal express the opinions of their authors and do not represent the opinion of the Journal, and the author of the research or study bears legal responsibility for this.

9) The works sent to the Journal are not returned to their authors, whether accepted for publication in the journal or not.

Terms and Ethics of Publication

Conditions et Ethique de Publication

رقم الإيداع بدار الكتب القطرية
2025 / 569

الترقيم الدولي الموحد للكتاب - ISBN
9789927124877

مركز البحوث والدراسات الأمنية
Center for Security Research & Studies

أكاديمية الشرطة
Police Academy

جميع حقوق النشر والتوزيع محفوظة
لمركز البحوث والدراسات الأمنية - أكاديمية الشرطة

للاطلاع على أعداد المجلة
والدليل الإسترشادي وشروط النشر
امسح الرمز أدناه