المجلة الليبية للدراسات الأكاديمية المعاصرة (Libyan Journal of Contemporary Academic Studies)
LJCAS, eISSN: 5970-3005
Volume 4, Issue 1, 2026, Pages: 66-82

# Cybersecurity Governance and Protection of Libyan National Identity: An Analytical Study of the Libyan Civil Registry Authority

Abdulhakim Abduazez Benjreid Ageel*
Department of Public Administration, Faculty of Economics and Political Science, Bani Waleed University, Bani Walid, Libya
*Corresponding author: hakimbenjaraid@bwu.edu.ly

# حوكمة الأمن السيبراني وحماية الهوية الوطنية الليبية: دراسة تحليلية على مصلحة الأحوال المدنية الليبية

أ. عبد الحكيم عبد العزيز بن جريد عقيل *
قسم الادارة العامة، كلية الاقتصاد والعلوم السياسية، جامعة بني وليد، بني وليد، ليبيا

**Received:** 06-11-2025; **Accepted:** 13-01-2026; **Published:** 26-01-2026

**Abstract:**
"This study examines cybersecurity governance as a fundamental pillar for safeguarding national identity and sovereign databases within the Libyan Civil Status Authority. It highlights the risks posed by digital threats and the phenomenon of fraudulent birth registration (commonly referred to as 'paper children'), resulting from legislative gaps, fragile technical infrastructure, and the exploitation of child allowance benefits. The study concludes that any compromise to data integrity constitutes a direct threat to national security. Accordingly, it recommends the adoption of a comprehensive national strategy and the implementation of a secure, integrated electronic linkage system.

**Keywords:** Cybersecurity Governance ،Digital National Identity ،Libyan Civil Status Authority ،National Security ،Sovereign Databases ،Digital Forgery (Paper Children) ،Digital Sovereignty.

**الملخص :**
تتناول الدراسة حوكمة الأمن السيبراني كركيزة لحماية الهوية الوطنية وقواعد البيانات السيادية بمصلحة الأحوال المدنية الليبية. تكشف عن مخاطر التهديدات الرقمية وتسجيل مواليد غير رسمي (أبناء من ورق) الناتج عن ضعف التشريعات وهشاشة البنية التقنية واستغلال قيمة علاوة الأبناء. تخلص إلى أن المساس بالبيانات يهدد الأمن القومي، وتوصي باستراتيجية وطنية وربط إلكتروني آمن.

**الكلمات المفتاحية:** حوكمة الأمن السيبراني، الهوية الوطنية الرقمية، مصلحة الأحوال المدنية الليبية، الأمن القومي، قواعد البيانات السيادية، التزوير الرقمي (أبناء من ورق).

## المقدمة

أصبحت الهوية الوطنية في العصر الرقمي إحدى الركائز الأساسية للأمن القومي للدول، لا سيما في ظل الاعتماد المتزايد على النظم المعلوماتية وقواعد البيانات الرقمية في إدارة شؤون المواطنين، وتقديم الخدمات العامة، وبناء السياسات الوطنية (Anderson, 2016). ولم تعد التهديدات التي تواجه الدول مقتصرة على الجوانب العسكرية التقليدية، بل امتدت لتشمل الفضاء السيبراني، الذي بات ساحة مفتوحة للاختراق والتلاعب والتزوير، خصوصًا في الدول التي تعاني من هشاشة مؤسساتية وضعف في أطر الحوكمة (Scrut, 2025scrut.io).

وفي هذا السياق، تُعد قواعد بيانات الأحوال المدنية من أخطر وأهم القواعد السيادية، نظرًا لارتباطها المباشر بالهوية الوطنية، والجنسية، والتركيبة الديموغرافية، والحقوق السياسية والاقتصادية والاجتماعية للأفراد (Elaswad & Jensen, 2016). ويؤدي أي خلل في إدارة هذه القواعد أو ضعف في حمايتها السيبرانية إلى تهديد مباشر للأمن القومي، ويُسهم في انتشار ظواهر خطيرة، مثل تزوير الهويات، والتلاعب بالسجلات، وتسجيل وقائع مدنية غير صحيحة (HoR Defense Committee, 2025libyaobserver.ly).

وتواجه الدولة الليبية، في ظل الانقسام المؤسسي والفراغ التشريعي والتقني، تحديات جسيمة في مجال حماية الهوية الوطنية الرقمية، حيث برزت إشكاليات متعددة، من أبرزها تسجيل المواليد دون ثبوت حالة وضع قانونية، الأمر الذي فتح المجال أمام التلاعب بالسجلات المدنية، وخلق واقعًا ديموغرافيًا مصطنعًا، بما يشكله ذلك من تهديد مباشر للأمن القومي الليبي (Libyan Prosecutors Uncover Large-Scale Identity Manipulation, 2025libyareview.com).

وانطلاقًا من ذلك، تبرز أهمية حوكمة الأمن السيبراني كإطار شامل يهدف إلى تنظيم السياسات، وتحديد المسؤوليات، وضبط العمليات التقنية والبشرية، بما يضمن حماية قواعد البيانات السيادية، ويحد من المخاطر السيبرانية التي تستهدف الهوية الوطنية (Calder, 2018). وتسعى هذه الدراسة إلى تحليل دور حوكمة الأمن السيبراني في مواجهة هذه المخاطر، من خلال دراسة تطبيقية على مصلحة الأحوال المدنية الليبية (Hackers attack Libya's civil registry database, 2016libyaobserver.ly).

**المشكلة البحثة:**

تتمثل مشكلة البحث في ضعف تطبيق مبادئ حوكمة الأمن السيبراني داخل مصلحة الأحوال المدنية الليبية، وما يترتب على ذلك من مخاطر تهدد سلامة قواعد بيانات الهوية الوطنية، وتفتح المجال أمام التلاعب والتزوير، خاصة فيما يتعلق بإشكالية تسجيل المواليد دون حالة وضع رسمية (حقيقية). وقد أفرز هذا الخلل جملة من الإشكاليات الخطيرة، من بينها:

- إدراج بيانات غير صحيحة ضمن السجل المدني.
- منح أرقام وطنية وهويات قانونية لأشخاص لا تنطبق عليهم الشروط القانونية، مدفوعاً في كثير من الحالات باستغلال قيمة علاوة الأبناء المالية.
- التأثير على التركيبة السكانية والسياسية والاقتصادية للدولة.
- تهديد منظومة الأمن القومي الليبي على المدى القريب والبعيد.

وعليه، تتبلور مشكلة البحث في السؤال الرئيس الآتي:

إلى أي مدى تسهم حوكمة الأمن السيبراني في الحد من مخاطر تهديد الهوية الوطنية الليبية وقواعد بياناتها، في ظل التحديات التي تواجه مصلحة الأحوال المدنية، وبخاصة إشكالية تسجيل المواليد دون حالة وضع؟

**ينبثق عن السؤال الرئيس** مجموعة من الأسئلة الفرعية:

- ما مفهوم حوكمة الأمن السيبراني، وما أهم أبعادها ومبادئها؟
- ما طبيعة المخاطر السيبرانية التي تواجه قواعد بيانات الأحوال المدنية الليبية؟
- كيف يسهم ضعف الحوكمة في تفاقم إشكالية تسجيل المواليد دون حالة وضع؟
- ما انعكاسات هذه الإشكالية على الأمن القومي الليبي؟
- ما مدى فاعلية الحلول المقترحة، مثل: تكليف الباحث الاجتماعي بالحصر الميداني للمواطنين وإعادة العمل بمنظومة البصمة الوراثية DNA.

**أهداف البحث:**

- توضيح الإطار المفاهيمي لحوكمة الأمن السيبراني.
- تحليل واقع حماية الهوية الوطنية وقواعد البيانات في مصلحة الأحوال .
- إبراز المخاطر المترتبة على تسجيل المواليد دون حالة وضع.
- بيان العلاقة بين أمن البيانات المدنية والأمن القومي الليبي.
- اقتراح حلول عملية قائمة على الحوكمة، من بينها التحقق الميداني ومنظومة الـ DNA.

**أهمية البحث :**

**الأهمية العلمية:**

- إثراء الأدبيات العربية في مجال حوكمة الأمن السيبراني.
- ربط مفهوم الأمن السيبراني بقضية الهوية الوطنية والأمن القومي.

**الأهمية العملية:**

- مساعدة صانعي القرار في مصلحة الأحوال المدنية.
- تقديم حلول قابلة للتطبيق للحد من التلاعب بالبيانات .
- دعم جهود الدولة في حماية الهوية الوطنية.

**فرضيات البحث :**

**الفرضية الرئيسة:** "هناك علاقة طردية ذات دلالة إحصائية وقانونية بين ضعف تطبيق حوكمة الأمن السيبراني في مصلحة الأحوال المدنية وبين تنامي التهديدات التي تمس الهوية الوطنية والأمن القومي الليبي".

**الفرضيات الفرعية:**

**الفرضية الأولى** (الجانب التشريعي): يؤدي غياب إطار قانوني وطني متكامل للأمن السيبراني وحماية البيانات الشخصية في ليبيا إلى عجز المؤسسات السيادية عن ملاحقة الجرائم الرقمية والحد من التلاعب بقواعد البيانات .

**الفرضية الثانية** (الجانب التقني والإداري): تعتبر هشاشة البنية التحتية التقنية وغياب سياسات إدارة الصلاحيات (Access Control) داخل مصلحة الأحوال المدنية هي الثغرة الأساسية التي تسمح ببروز ظاهرة "أبناء من ورق" والتلاعب بالسجلات المدنية .

**الفرضية الثالثة** (الجانب الأمني): إن استهداف قواعد بيانات الهوية الوطنية لا يمثل مجرد خلل فني، بل هو أداة من أدوات الحروب غير التقليدية التي تستهدف تقويض السيادة الرقمية للدولة الليبية واستقرارها السياسي والاجتماعي .

**الفرضية الرابعة** (الجانب الإجرائي): تفعيل الربط الإلكتروني المباشر بين المؤسسات الصحية (المولدّة للبيانات) والسجل المدني وفق معايير حوكمة سيبرانية سيؤدي إلى القضاء على عمليات تسجيل المواليد غير الحقيقية بنسبة كبيرة .

**حدود البحث:**

**الحدود الموضوعية:** حوكمة الأمن السيبراني والهوية الوطنية .
**الحدود المكانية:** مصلحة الأحوال المدنية الليبية .
**الحدود الزمنية:** الفترة المعاصرة لتطور النظم الرقمية في ليبيا.

**منهجية البحث:**

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، مع الاستعانة بالمنهج المقارن، وذلك وفق التفصيل الآتي:

1. **المنهج الوصفي**: يستخدم لوصف الإطار المفاهيمي لحوكمة الأمن السيبراني، وتوضيح طبيعة الهوية الوطنية الرقمية وقواعد البيانات السيادية، بالإضافة إلى رصد واقع البنية التقنية والإدارية لمصلحة الأحوال المدنية في ليبيا .
2. **المنهج التحليلي**: يُستخدم لتحليل النصوص القانونية والتشريعات المنظمة للأمن السيبراني والأحوال المدنية، وتحليل العلاقة بين الثغرات التقنية (مثل ظاهرة "أبناء من ورق") وبين تهديدات الأمن القومي، مع تحليل انعكاسات هذه التهديدات على الاستقرار السياسي والاجتماعي.

3. **المنهج المقارن**: يُستخدم من خلال استعراض التجارب الدولية الرائدة (مثل تجربة الاتحاد الأوروبي GDPR، وتجربة إستونيا) في حوكمة الأمن الرقمي، للمقارنة بينها وبين الحالة الليبية واستنباط أفضل الممارسات التي يمكن تطبيقها لتعزيز الأمن السيبراني في ليبيا ).

**أدوات البحث**:

**المراجعة المكتبية:** الاعتماد على الكتب، الدوريات العلمية، التقارير الصادرة عن المؤسسات الدولية (مثل ITU وISACA)، والوثائق الرسمية الصادرة عن مصلحة الأحوال المدنية الليبية.

**تحليل المضمون:** تحليل القوانين والقرارات الوزارية الليبية المتعلقة بالتحول الرقمي والرقم الوطني لبيان أوجه القصور فيها.

## المبحث الأول الإطار المفاهيمي والنظري لحوكمة الأمن السيبراني

### المطلب الأول: مفهوم الحوكمة ومبادئها

#### أولًا: مفهوم الحوكمة

يُعد مفهوم الحوكمة (Governance) من المفاهيم الحديثة نسبيًا في الفكر الإداري والسياسي، وقد تبلور بصورة واضحة في أواخر القرن العشرين نتيجة التحولات البنيوية التي شهدها النظام الدولي، ولا سيما مع تصاعد العولمة، وتراجع الدور الاحتكاري للدولة، وبروز فاعلين جدد كالشركات متعددة الجنسيات والمنظمات الدولية، إلى جانب التطور المتسارع في تكنولوجيا المعلومات والاتصالات (Laudon & Laudon, 2020). وقد فرضت هذه التحولات ضرورة إيجاد آليات جديدة لإدارة الشأن العام تقوم على الشفافية والمساءلة والكفاءة بدلًا من الأساليب البيروقراطية التقليدية (What is Cyber Governance? - ZenGRC, 2022 zengrc.com). وتشير الحوكمة إلى منظومة متكاملة من القواعد والمؤسسات والآليات التي يتم من خلالها توجيه السلطة وممارسة الرقابة على الأداء المؤسسي، بما يحقق الاستخدام الأمثل للموارد ويحافظ على التوازن بين السلطات المختلفة (Cybersecurity Governance - CISA, n.d.cisa.gov). وفي هذا السياق، عرّف البنك الدولي الحوكمة بأنها: «الطريقة التي تُمارس بها السلطة في إدارة الموارد الاقتصادية والاجتماعية للدولة من أجل تحقيق التنمية (Understanding NIST Cybersecurity Framework (CSF) 2.0 in 2026, 2025 techdemocracy.com). ويُفهم من هذا التعريف أن الحوكمة ترتبط ارتباطًا وثيقًا بفعالية السياسات العامة وجودة المؤسسات (What Is Cybersecurity Governance? - Mimecast, n.d.mimecast.com). كما عرّف برنامج الأمم المتحدة الإنمائي الحوكمة بأنها: «ممارسة السلطة السياسية والاقتصادية والإدارية لإدارة شؤون الدولة على جميع المستويات، وتشمل الآليات والعمليات التي يتم من خلالها التعبير عن مصالح المواطنين وممارسة حقوقهم القانونية» (World Economic Forum, 2020num.univ-msila.dz). ويؤكد هذا التعريف البعد التشاركي للحوكمة، ودورها في تعزيز سيادة القانون وحماية الحقوق والحريات (What is a Cybersecurity Governance Framework? - Portnox, n.d.portnox.com). ومن خلال هذه التعريفات، يتضح أن الحوكمة مفهوم شامل يتجاوز الإدارة التقليدية ليشمل الأبعاد السياسية والتشريعية والرقابية، وهو ما يجعلها إطارًا مناسبًا لمعالجة القضايا المعقدة، ومن بينها قضايا الأمن السيبراني (Common Cyber Governance Principles and Standards, n.d. link.springer.com).

#### ثانيًا: مبادئ الحوكمة

تقوم الحوكمة على مجموعة من المبادئ الأساسية التي تشكل مرجعًا معياريًا لتقييم الأداء المؤسسي، ومن أبرزها: الشفافية: وتعني إتاحة المعلومات ذات الصلة بوضوح ودقة وفي الوقت المناسب لجميع أصحاب المصلحة. المساءلة: خضوع صناع القرار والقائمين على الإدارة للمحاسبة القانونية والمؤسسية. سيادة القانون: الالتزام بالقوانين والتشـــريعات وتطبيقها بعدالة دون تمييز. الكفاءة والفعالية: تحقيق الأهداف بأفضل استخدام ممكن للموارد. المشاركة: إشراك المواطنين وأصحاب المصلحة في عملية صنع القرار (Cybersecurity governance: Meaning, importance, elements, process - Scrut, 2025 scrut.io). وتُعد هذه المبادئ حجر الأساس لأي نموذج حوكمة ناجح، كما تمثل الإطار المرجعي لتطبيق

الحوكمة في القطاعات التقنية والرقمية، وبخاصة في مجال الأمن السيبراني الذي يتطلب مستويات عالية من التنسيق والشفافية (The Top Security, Risk, and AI Governance Frameworks CISOs Must Prioritize for 2026, n.d.cybersaint.io).

**المطلب الثاني: حوكمة الأمن السيبراني – المفهوم والأبعاد**

**أولًا:** مفهوم **الأمن السيبراني**

يُعد الأمن السيبراني أحد الركائز الأساسية للأمن القومي في العصر الرقمي، نظرًا لاعتماد الدول المتزايد على البنى التحتية الرقمية في إدارة المرافق الحيوية، مثل الطاقة، والمصارف، والاتصالات، والخدمات الحكومية (Stallings & Brown, 2018). ويشير مفهوم الأمن السيبراني إلى حماية الأنظمة المعلوماتية والشبكات وقواعد البيانات من التهديدات الإلكترونية، سواء كانت جرائم سيبرانية، أو هجمات منظمة، أو أعمال تجسس رقمي .(Cybersecurity Framework Guide 2026, 2023sprintzeal.com) ويعرّف Knapp وFerrante الأمن السيبراني بأنه: «مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية الفضاء السيبراني ومكوناته من التهديدات والمخاطر المحتملة».(Cordesman, 2019) كما عرّف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه: «مجموعة الأدوات والسياسات والمفاهيم الأمنية والتدابير والمبادئ التوجيهية التي تُستخدم لحماية الأصول الرقمية والبنية التحتية للمعلومات» (International Telecommunication Union, 2024libyareview.com). وتبرز أهمية هذه التعريفات في تأكيدها على أن الأمن السيبراني ليس مسألة تقنية بحتة، بل قضية استراتيجية متعددة الأبعاد تشمل الجوانب القانونية والمؤسسية والبشرية (Kraemer et al., 2009).

**ثانيًا: مفهوم حوكمة الأمن السيبراني**

يقصد بحوكمة الأمن السيبراني الإطار المؤسسي والاستراتيجي الذي يحدد كيفية إدارة المخاطر السيبرانية، وتوزيع الصلاحيات والمسؤوليات، وصياغة السياسات والتشريعات، بما يضمن حماية الأصول الرقمية وتحقيق الأهداف الاستراتيجية للدولة أو المؤسسة (What is Cyber Governance? - ZenGRC, 2022zengrc.com).

وتعرّف منظمة ISACA حوكمة الأمن السيبراني بأنها: «نظام يتم من خلاله توجيه ومراقبة الأمن السيبراني لضمان توافقه مع أهداف المنظمة وإدارة مخاطره بفعالية» (ISO, 2018). وبناءً على ذلك، فإن حوكمة الأمن السيبراني تشمل عدة أبعاد متكاملة، من أبرزها: القيادة العليا وصنع القرار الاستراتيجي ، الإطار التشريعي والتنظيمي ، السياسات والإجراءات التشغيلية العنصر البشري وبناء القدرات ، إدارة المخاطر والاستجابة للحوادث (Understanding NIST Cybersecurity Framework (CSF) 2.0 in 2026, 2025 techdemocracy.com).

**ثالثًا: الأطر القانونية المقارنة لحوكمة الأمن السيبراني**

اعتمدت العديد من الدول أطرًا قانونية متقدمة لحوكمة الأمن السيبراني. فعلى سبيل المثال، أقرّ الاتحاد الأوروبي اللائحة العامة لحماية البيانات (GDPR) التي وضعت معايير صارمة لحماية البيانات الشخصية، وفرضت التزامات واضحة على المؤسسات بشأن إدارة المخاطر والإبلاغ عن الحوادث السيبرانية (European Union Agency for Cybersecurity, 2024techdemocracy.com). وفي الولايات المتحدة، اعتمد المعهد الوطني للمعايير والتكنولوجيا إطار NIST للأمن السيبراني، الذي يركز على الحوكمة القائمة على إدارة المخاطر، ويُعد نموذجًا مرجعيًا تستخدمه المؤسسات الحكومية والخاصة (Cybersecurity Framework | NIST, n.d.nist.gov). أما تجربة إستونيا، فتُعد من أبرز التجارب الدولية، حيث أنشأت بنية تشريعية ومؤسسية متكاملة للأمن السيبراني عقب الهجمات السيبرانية التي تعرضت لها عام 2007، وركزت على التكامل بين الحكومة والقطاع الخاص وبناء الثقة الرقمية (Heeks, 2017). رابعًا: أهداف حوكمة الأمن السيبراني تهدف حوكمة الأمن السيبراني إلى تحقيق مجموعة من الأهداف الاستراتيجية، من أبرزها: حماية الأصول الرقمية السيادية والبنية التحتية الحيوية ،ضمان استمرارية الأعمال والخدمات

الحكومية. الحد من المخاطر السيبرانية وتقليل آثار الهجمات. ، تعزيز الثقة في النظم الرقمية والتعاملات الإلكترونية دعم الأمن القومي وتحقيق الاستقرار الرقمي للدولة .(Turban et al., 2018)

**المطلب الثالث: الهوية الوطنية الرقمية وقواعد البيانات السيادية**

**أولًا: الإطار القانوني للهوية الوطنية والرقمية**

الهوية الوطنية، في جوهرها، هي صك قانوني يربط الفرد بالدولة ومن خلالها تُمارَس الحقوق السياسية والاجتماعية والاقتصادية (الزاوي, 2016). ومع التحول الرقمي، تحولت هذه الهوية إلى هوية وطنية رقمية ذات طابع قانوني وسياسي تُخزَّن وتُدار إلكترونيًا عبر قواعد بيانات مركزية أو موزعة، ممّا استلزم تطوير أطر تشريعية متخصصة لحماية هذه البيانات وتنظيمها .(NCSI Libya, n.d.ncsi.ega.ee) في العديد من الدول، تم إدراج الهوية الرقمية صراحة في التشريعات الوطنية كجزء من قانون الهوية الرقمية والتوقيع الإلكتروني الذي ينظم آليات المنح، الاستخدام، السلامة القانونية، والآثار القانونية للمعاملات الرقمية (قانون الهوية الرقمية والتوقيع الإلكتروني، eID + Trust Services Law) (Data protection laws in Libya, 2024dlapiperdataprotection.com). هذا النوع من التشريعات أنشأ في عدة أنظمة قانونية إطارًا طويل الأمد لحماية بيانات المواطنين وحفظ سيادة الدولة على قواعد البيانات السيادية. من منظور قانوني، تُعد قوانين حماية البيانات (مثل اللائحة العامة لحماية البيانات – GDPR في الاتحاد الأوروبي) حجر الزاوية في ضمان الحقوق الأساسية للمواطنين، إذ تفرض قيوداً على معالجة البيانات الشخصية، وتنظيم التحقق من الهويات، وتحدد شروط نقل البيانات خارج الدول أو المنظمات الدولية، ما يعزز سيادة الدولة الرقمية ويحمي خصوصية الأفراد (European Union Agency for Cybersecurity, 2024techdemocracy.com). مثال قانوني تطبيقي: في التشريع الأوروبي، يُلزم القانون المؤسسات الحكومية والخاصة باحترام قواعد حماية البيانات الشخصية ومعاييرها، ما يجعل أي نظام هوية رقمية يرتبط بقواعد صارمة لضمان حقوق الخصوصية والشفافية القانونية (Gibson Dunn, 2024zengrc.com).

**ثانيًا: قوانين حماية قواعد البيانات السيادية**

قواعد البيانات السيادية (مثل سجلات الأحوال المدنية، الجوازات، الرقم الوطني) تحتل مرتبة خاصة في المنظومة القانونية، لأنها تضم معلومات استراتيجية لمسار الدولة وأمنها القومي (المرغني, 2020). من الناحية القانونية، تخضع هذه القواعد إلى أطر حماية البيانات، قوانين مكافحة الجرائم الإلكترونية، وأحيانًا قوانين خاصة بحماية البنى التحتية الحيوية (Critical Infrastructure Protection) (Libya: Revoke Repressive Anti-Cybercrime Law, 2023hrw.org). لذلك، في التشريعات المقارنة، يتم التفريق بين: البيانات العادية – تخضع لقانون حماية البيانات الشخصية. البيانات السيادية الاستراتيجية – تُعامَل كجزء من البنية التحتية الحيوية، وتُفرض عليها قواعد صارمة في التحكم، الترخيص، والتنظيم. في بعض التشريعات المقترحة (مثل المشاريع في العراق)، يتم تأسيس قوانين متكاملة تشمل: قانون الحوكمة الشاملة للبيانات (Data Governance Law) لتنظيم ملكية الدولة على البيانات الحكومية. قانون الأمن السيبراني الوطني لحماية قواعد البيانات الحيوية من التهديدات التقنية. قانون الهوية الرقمية والتوقيع الإلكتروني كإطار قانوني للثقة الرقمية .(Majid, 2022)

**ثالثًا: مقارنة تجريبية بين تجارب دولية في الهوية الرقمية في التحليل المقارن**

أظهرت دراسات متخصصة أن الدول تختلف في كيفية تأسيس أطرها القانونية للهوية الرقمية: الاتحاد الأوروبي: نظام eIDAS يُعدّ من أقدم الإطارات القانونية للهوية الرقمية، حيث يوفر معايير موحدة للاعتراف بالهوية الإلكترونية والتوقيعات الرقمية عبر دول التكتل، ما يُعزّز الأمن القانوني للطرفين (الدولة والمواطن) في المعاملات الرقمية (U.S. Department of Justice, 2024etico.iiep.unesco.org). التجارب الوطنية في آسيا وشمال أوروبا: بعض الدول تبنت نماذج الهوية الرقمية ذاتية السيادة (Self-Sovereign Identity – SSI) القائمة على مبادئ اللامركزية والسيطرة الشخصية على البيانات، وذلك لتقليل الاعتماد على قواعد بيانات مركزية موحدة. تُبرز دراسة

تحليلية مقارنة أن هذه النماذج توفر حماية أفضل من اختراقات البيانات وتعزز سيادة المواطن على بياناته (Heeks, 2017). التجارب المقترحة في العالم العربي: أشار النقد القانوني إلى أن غياب إطار قانوني واضح للهوية الرقمية يجعل البلدان أكثر عرضة لانتهاكات الحق في الخصوصية وتعريض قواعد البيانات الوطنية للمخاطر القانونية في حالات تسرب البيانات أو سوء إدارتها في ظل عدم وضوح نصوص العقوبات والإجراءات (العرفي, 2019). المطلب الرابع: العلاقة بين حوكمة الأمن السيبراني والأمن القومي – تحليل قانوني ومقارن أولًا: الأمن السيبراني كجزء من القانون الوطني لقد ثبت أن الأمن السيبراني لم يعد مجرد مسألة تقنية، بل أصبح أولوية قانونية وسياسية ترتبط بحماية أفراد المجتمع، المؤسسات، والبنى التحتية الحيوية، ومن بينها قواعد الهوية الرقمية (Libyan National Information Security & Safety Authority, 2022thearabweekly.com). في كثير من التشريعات، يدخل الأمن السيبراني ضمن قانون حماية البينة التحتية الحيوية الذي يفرض التزامات قانونية على الجهات الحكومية والخاصة لحماية نظم المعلومات، ومنع التهديدات أو الاختراقات التي قد تكون لها آثار على الأمن القومي (Libya Still Mired in Political Deadlock, 2025press.un.org). من منظور قانوني دولي، تُعَدّ السيادة الرقمية للدولة محورًا جديدًا في القانون الدولي العام، حيث يُنظر إلى الفضاء السيبراني كجزء من نطاق السيادة الوطنية، ويُطلب تطوير قواعد قانونية مرنة لمواجهة التهديدات السيبرانية التي لا تلتزم بالحدود الجغرافية التقليدية (Libya Political Risk Report, 2026thegeopoliticaldesk.com). ثانيًا: التكامل بين الأمن السيبراني والهوية الرقمية في القانون المقارن إن حوكمة الأمن السيبراني في النظم القانونية المتقدمة تشمل عادة: إطارًا تشريعيًا موحدًا لحماية البنية التحتية الحيوية الرقمية ، تحديد صلاحيات الجهات الرقابية والتنسيق بينها (مثل وحدات الاستجابة للحوادث – CERT/SOC) ، عقوبات جنائية مدرجة في قوانين الجرائم الإلكترونية لحماية قواعد البيانات الوطنية ومنع التلاعب بها .(Muhammad, 2025) في الاتحاد الأوروبي وضمن إطار 2NIS وGDPR، تنص التشريعات على متطلبات إلزامية للإبلاغ عن الانتهاكات الأمنية، تقييم المخاطر، وضمان شفافية المعالجة، ما يساعد على ربط الأمن السيبراني بالحقوق الأساسية للمواطنين .(European Union Agency for Cybersecurity, 2024techdemocracy.com)

**خلاصة المبحث الاول**

- الهوية الوطنية الرقمية يجب أن تكون مدعومة بقوانين واضحة تحدد المسؤوليات، حدود الوصول، وتضمن حقوق الأفراد في الخصوصية والمعالجة الآمنة للبيانات ( Data Privacy Day: As Libya Goes Digital, Trust Becomes the Foundation, n.d.libyanspider.com).
- قواعد البيانات السيادية تُعد جزءًا من البنية التحتية الحيوية التي تستوجب حماية قانونية تقنية مضاعفة، تشمل عقوبات رادعة وتنظيمات تشغيلية صارمة (Libya uncovers mass identity fraud, 2025thearabweekly.com).
- التجارب الدولية تظهر تنوع النماذج القانونية (الأطر الموحدة مثل eIDAS مقابل نماذج الهوية الذاتية السيادية)، ويتضح أنه كلما كانت القاعدة القانونية أكثر تحديدًا وحماية، كانت الدولة في موقع أفضل لمواجهة التهديدات السيبرانية وحماية السيادة الوطنية (U.S. Department of Justice, 2024etico.iiep.unesco.org).
- حوكمة الأمن السيبراني يجب أن تُدمج في القانون الوطني بحيث تشمل الاستجابة للطوارئ، تقييم المخاطر، حماية البيانات، وتنسيق سلطات تنفيذية وقضائية ( Libyan National Information Security & Safety Authority, 2024thearabweekly.com).

**المبحث الثاني: الهوية الوطنية الليبية ومصلحة الأحوال المدنية الإطار التنظيمي والتقني**

**المطلب الأول: تطور الهوية الوطنية في ليبيا**

**أولًا: الهوية الوطنية في الإطار القانوني الليبي**

تُعد الهوية الوطنية في ليبيا أحد المرتكزات الأساسية لبناء الدولة الحديثة، إذ ترتبط ارتباطًا وثيقًا بمفاهيم السيادة، والمواطنة، والانتماء القانوني (الزاوي, 2016). وقد اهتم المشرّع الليبي بتنظيم مسائل الجنسية والأحوال المدنية منذ فترات مبكرة، إدراكًا لأهميتها في ضبط العلاقة بين الفرد والدولة (Libya trapped

in a cycle of political crisis, 2025gisreportsonline.com). وقد صدر قانون الجنسية الليبية رقم (17) لسنة 1954، والذي شكّل الإطار القانوني الأول المنظم لمسألة الانتماء الوطني، محددًا شروط اكتساب الجنسية وفقدانها. كما صدرت لاحقًا تشريعات منظمة للأحوال المدنية، هدفت إلى تسجيل الوقائع الحيوية للمواطنين، مثل الميلاد، والزواج، والوفاة، بما يضمن تثبيت الوضع القانوني للفرد داخل المجتمع (العرفي, 2019). غير أن هذه التشريعات، رغم أهميتها، لم تُواكب في كثير من الأحيان التطورات التقنية المتسارعة، ولم تُدعَّم بإجراءات حوكمة فعالة، الأمر الذي أفرز ثغرات قانونية وإدارية، استُغلت لاحقًا في التلاعب بالهوية الوطنية .(HoR Defense Committee, 2025libyaobserver.ly)

**ثانيًا: التحول من الهوية الورقية إلى الهوية الرقمية**

شهدت ليبيا، أسوة بغيرها من الدول، تحولًا تدريجيًا من النظم الورقية التقليدية إلى النظم الرقمية في إدارة بيانات الأحوال المدنية، خاصة مع إدخال منظومة الرقم الوطني وقواعد البيانات الإلكترونية المركزية (Elaswad & Jensen, 2016). وقد هدف هذا التحول إلى: تسريع الإجراءات الإدارية ، تقليل الازدواجية في السجلات ، تعزيز دقة البيانات ، تحسين تقديم الخدمات للمواطنين. إلا أن هذا الانتقال لم يكن مصحوبًا بإطار متكامل لحوكمة الأمن السيبراني، مما جعل المنظومات الرقمية عرضة للاختراق وسوء الاستخدام، خاصة في ظل ضعف البنية التحتية التقنية، وغياب التدريب المتخصص للكوادر البشرية Hackers attack Libya's civil registry database, 2016libyaobserver.ly).)

**المطلب الثاني: مصلحة الأحوال المدنية الليبية – النشأة والاختصاصات**

**أولًا: النشأة القانونية لمصلحة الأحوال المدنية**

تُعد مصلحة الأحوال المدنية الجهة الرسمية المختصة بتسجيل وتوثيق الوقائع المدنية للمواطنين الليبيين، تسجيل المواليد ، تسجيل الوفيات ، اصدار الارقام الوطنية ، الزواج والطلاق ،إدارة قواعد بيانات الهوية الوطنية (المرغني, 2020). وقد أُنشئت المصلحة بموجب تشريعات تنظيمية تهدف إلى توحيد السجلات المدنية وضمان دقتها، باعتبارها المرجع الأساسي لكافة مؤسسات الدولة. وقد تأسست مصلحة الأحوال المدنية الليبية رسمياً كشخصية اعتبارية مستقلة بموجب القرار رقم (115) لسنة 1998م الصادر عن اللجنة الشعبية العامة، لتتولى تنظيم وتسجيل واقعات الأحوال المدنية (ولادة ، زواج ، طلاق ، وفاة) وإصدار كتيب العائلة والوثائق الرسمية ، تتبعها فروع ومكاتب في كافة أنحاء ليبيا. النشأة والتطور القانوني: البداية (1968): تم إرساء الأساس القانوني لتسجيل الأحوال المدنية بصدور القانون رقم (36) لسنة 1968م، الذي أقر بإنشاء مكاتب للسجل المدني في كل بلدية. التعديل والتنظيم (1988): صدر القانون رقم (7) لسنة 1988م لتعديل أحكام القانون رقم 36 لسنة 1968، مؤكداً حجية سجلات الأحوال المدنية في البيانات الشخصية. التأسيس الفعلي (1998): صدر القرار رقم 115 لسنة 1998م بإنشاء المصلحة ككيان إداري مستقل ، وتبعه قرار آخر بإنشاء فروع المصلحة وتحديد اختصاصاتها. التحول الرقمي (2014): صدر القانون رقم (8) لسنة 2014 بشأن الرقم الوطني، الذي جعل من قاعدة بيانات المصلحة حجر الزاوية للمواطنة والخدمات العامة (Elaswad & Jensen, 2016). تتمتع المصلحة بذمة مالية مستقلة ، وتهدف إلى توثيق الحالة المدنية لليبيين والأجانب ، وتعمل وفقاً للتشريعات النافذة وقوانين (Data protection laws in Libya, 2024dlapiperdataprotection.com).

**ثانيًا: الاختصاصات السيادية لمصلحة الأحوال المدنية**

تكتسب مصلحة الأحوال المدنية صفة المؤسسة السيادية ، نظرًا لارتباط مهامها المباشر بالأمن القومي ، حيث تعتمد عليها مؤسسات حيوية ، مثل: الأجهزة الأمنية ، المفوضية الوطنية العليا للانتخابات ، المصارف، مؤسسات التعليم والصحة ، وأي خلل في بيانات المصلحة ينعكس بصورة مباشرة على: نزاهة العمليات الانتخابية ، توزيع الدعم والخدمات ، ضبط التركيبة السكانية ، حماية السيادة الوطنية (Cordesman, 2019).

**المطلب الثالث: البنية التقنية لقواعد بيانات الأحوال المدنية**

**أولًا: مكونات المنظومة المعلوماتية**

تعتمد مصلحة الأحوال المدنية على منظومة معلوماتية مركزية، تتكون من: قواعد بيانات رقمية ، شبكات اتصال داخلية وخارجية ، أنظمة تحقق وهوية ، صلاحيات وصول للمستخدمين. وتمثل هذه المنظومة العمود الفقري لإدارة الهوية الوطنية الرقمية، ما يجعلها هدفًا مباشرًا للهجمات السيبرانية أو التلاعب الداخلي (Hackers attack Libya's civil registry database, 2016libyaobserver.ly).

**ثانيًا: التحديات التقنية والأمنية**

تواجه المنظومة التقنية لمصلحة الأحوال المدنية عدة تحديات، من أبرزها: ضعف أنظمة التشفير والحماية. ، غياب المراجعة الدورية للصلاحيات ، الاعتماد على العنصر البشري غير المؤهل أحيانًا ، ضعف التكامل بين المنظومات المختلفة ، غياب خطط الاستجابة للحوادث السيبرانية (Turmoil in Libya: Major Industries Hit by Massive DDoS Attacks, 2023nsfocusglobal.com). وتؤدي هذه التحديات إلى ارتفاع احتمالات: اختراق البيانات ، التلاعب بالسجلات ، إدخال بيانات غير صحيحة (Libyan Prosecutors Uncover Large-Scale Identity Manipulation, 2025libyareview.com).

**المطلب الرابع: إشكالية تسجيل المواليد دون حالة وضع رسمية(حقيقية)**

**أولًا: مفهوم حالة الوضع وأهميتها القانونية**

يُعد تسجيل المواليد أحد الركائز الأساسية لضمان الحقوق القانونية والإنسانية للأفراد، إذ يمنح الطفل هوية قانونية تمكّنه من التمتع بحقوقه في التعليم، والرعاية الصحية، والحماية الاجتماعية (Albrecht et al., 2018). إلا أن بعض الدول، ومن بينها ليبيا، شهدت خلال السنوات الأخيرة إشكاليات خطيرة تتعلق بتسجيل مواليد دون وجود حالة وضع رسمية حقيقية، بل ورُصدت حالات تسجيل مواليد غير موجودين فعليًا، فيما يمكن تسميته بظاهرة "أبناء من ورق" (Libya uncovers mass identity fraud, 2025thearabweekly.com).

**ثانياً: ماهية الإشكالية**

تتمثل الإشكالية في تسجيل مواليد في السجلات المدنية دون: وجود ولادة حقيقية مثبتة طبيًا أو دون استيفاء الإجراءات القانونية المعتمدة ، أو عبر استغلال ثغرات إدارية وضعف الرقابة وهو ما يؤدي إلى خلق هويات قانونية لأشخاص غير موجودين على أرض الواقع (Public Prosecution: Forgery of 16 family records, n.d.facebook.com).

**ثالثاً: أسباب الظاهرة**

من أبرز الأسباب التي ساهمت في انتشار هذه الظاهرة: ضعف منظومة السجل المدني والرقابة الإدارية ، الفساد الإداري واستغلال النفوذ ، النزاعات المسلحة وحالة الانقسام المؤسسي ، استخدام هذه التسجيلات لأغراض غير مشروعة (م...(truncated 5107 characters)...فيات. ومع تزايد التهديدات السيبرانية، بات استهداف هذه المؤسسة يشكل خطرًا مباشرًا على الأمن القومي الليبي بأبعاده المختلفة (Civil Conflict in Libya, 2024cfr.org).

**رابعا: التهديدات السيبرانية لمصلحة الأحوال المدنية**

تشمل التهديدات السيبرانية المحتملة: اختراق قواعد البيانات والتلاعب بالمعلومات ، تزوير أو حذف أو إضافة قيود وهمية ، سرقة البيانات وبيعها أو استخدامها لأغراض غير مشروعة ، تعطيل الأنظمة (الهجمات التخريبية – الحرمان من الخدمة) ، اختراق داخلي نتيجة ضعف الضوابط أو الفساد (Hackers attack Libya's civil registry database, 2016libyaobserver.ly).

**خامسا: انعكاسات التهديدات السيبرانية على السيادة الوطنية**

تمثل بيانات الأحوال المدنية جزءًا لا يتجزأ من السيادة الوطنية، وأي اختراق لها يؤدي إلى: المساس بقدرة الدولة على التحكم في بيانات مواطنيها ، فقدان الثقة في مؤسسات الدولة السيادية إمكانية تدخل أطراف خارجية في الشأن الداخلي عبر التحكم أو التلاعب بالبيانات ، إضعاف مفهوم الهوية الوطنية القانونية ، وبذلك تتحول الهجمات السيبرانية إلى أداة من أدوات الحرب غير التقليدية ضد الدولة الليبية (Libya Still Mired in Political Deadlock, 2025press.un.org).

**سادسا: انعكاساتها على الاستقرار السياسي**

يؤدي اختراق بيانات الأحوال المدنية إلى: التلاعب بقوائم الناخبين والعملية الانتخابية ،خلق نزاعات قانونية حول الجنسية والهوية ،توظيف البيانات المزورة في الصراع السياسي ، تعميق الانقسام وفقدان الثقة في نتائج الاستحقاقات السياسية ، وهو ما يهدد مسار بناء الدولة والاستقرار السياسي (Libya Political Risk Report, 2026thegeopoliticaldesk.com).

**سابعاً: انعكاساتها على الاستقرار الاجتماعي**

على المستوى الاجتماعي، تؤدي هذه التهديدات إلى: انتشار الهويات الوهمية وما يُعرف بـ"الأشخاص غير الحقيقيين" ، النزاعات الأسرية والقانونية حول النسب والحالة الاجتماعية ، الإخلال بمبدأ العدالة في توزيع الخدمات ، فقدان ثقة المواطن في منظومة الدولة ومؤسساتها ، الأمر الذي ينعكس سلبًا على السلم الاجتماعي والتماسك المجتمعي .(Albrecht et al., 2018) سادساً: انعكاساتها على الأمن الاقتصادي تمثل بيانات الأحوال المدنية أساسًا للسياسات الاقتصادية، ويؤدي اختراقها إلى: الاستيلاء غير المشروع على المرتبات والدعم والإعانات ، تشويه الإحصاءات السكانية المؤثرة في التخطيط الاقتصادي ، زيادة الاقتصاد غير الرسمي ، استنزاف الموارد العامة وهدر المال العام كما قد تُستخدم البيانات المسروقة في عمليات غسل الأموال أو الاحتيال المالي (Libya Crisis Response Plan 2025 - 2026, 2025crisisresponse.iom.int).

**ثامناً:البعد الأمني والاستخباراتي**

تشكل قواعد بيانات الأحوال المدنية هدفًا استراتيجيًا للأجهزة الاستخباراتية المعادية، حيث يتيح اختراقها: بناء قواعد بيانات استخباراتية عن المجتمع الليبي ، تتبع الشخصيات المؤثرة أو استهدافها ، دعم شبكات الجريمة المنظمة والإرهاب (Situation in Libya at the International Criminal Court, n.d.ecchr.eu).

**المطلب الخامس: قصور تطبيق حوكمة الأمن السيبراني في ليبيا**

**أولاً: غياب الاستراتيجية الوطنية للأمن السيبراني**

يُعد غياب استراتيجية وطنية شاملة للأمن السيبراني من أبرز مظاهر قصور تطبيق حوكمة الأمن السيبراني في ليبيا. فالاستراتيجية الوطنية تمثل الإطار المرجعي الذي يحدد الرؤية العامة، والأهداف، والأدوار والمسؤوليات، وآليات التنسيق بين الجهات الحكومية والخاصة ذات العلاقة. وفي ظل غياب هذا الإطار، تعاني المؤسسات من العمل بشكل منفصل وردّ فعلي، دون توحيد للسياسات أو المعايير أو الأولويات (Al-Ali, 2021). كما يؤدي هذا الغياب إلى ضعف القدرة على إدارة المخاطر السيبرانية على المستوى الوطني، وغياب خطط واضحة للاستجابة للحوادث السيبرانية أو التعافي منها. إضافة إلى ذلك، يحدّ عدم وجود استراتيجية وطنية من فرص التعاون الدولي وتبادل الخبرات والمعلومات، ويجعل الدولة أقل جاهزية لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف البنية التحتية الحيوية والبيانات الحساسة (Libyan National Information Security & Safety Authority, 2022thearabweekly.com).

**ثانياً: ضعف الوعي والتدريب في مجال الأمن السيبراني**

يُعد ضعف الوعي والتدريب بالأمن السيبراني من العوامل الأساسية التي تعمّق قصور حوكمة الأمن السيبراني في ليبيا. فالعنصر البشري يمثل خط الدفاع الأول ضد الهجمات السيبرانية، إلا أن محدودية البرامج التدريبية وغياب حملات التوعية المنتظمة يؤديان إلى ارتفاع مستوى المخاطر الناتجة عن الأخطاء البشرية وسوء استخدام الأنظمة التقنية (Kraemer et al., 2009). كما يلاحظ نقص واضح في الكفاءات المتخصصة في مجال الأمن السيبراني، سواء على مستوى المؤسسات الحكومية أو القطاع الخاص، الأمر الذي ينعكس سلباً على قدرة هذه الجهات على تطبيق السياسات الأمنية ومراقبة الالتزام بها. ويؤدي ضعف التدريب أيضاً إلى عدم فهم القيادات الإدارية لأهمية حوكمة الأمن السيبراني ودورها في دعم استمرارية الأعمال وحماية الأصول الرقمية، مما يقلل من أولوية هذا المجال في التخطيط الاستراتيجي واتخاذ القرار (Libyan Government Trains Personnel in Electoral Cyber Threats, 2023darkreading.com).

**خلاصة المبحث الثاني**

خلص هذا الفصل إلى أن قواعد بيانات الأحوال المدنية الليبية تواجه مخاطر سيبرانية جسيمة، ناتجة عن هشاشة البنية التقنية، وضعف التشريعات، وقصور تطبيق حوكمة الأمن السيبراني، وأن إشكالية تسجيل المواليد دون حالة وضع تُعد أحد أخطر التهديدات غير المباشرة للهوية الوطنية والأمن القومي (Libya uncovers mass identity fraud, 202thearabweekly.com).

**المبحث الثلث: الدراسة التحليلية لواقع حوكمة الأمن السيبراني في مصلحة الأحوال المدنية الليبية.**

يهدف هذا الفصل إلى تحليل واقع حوكمة الأمن السيبراني داخل مصلحة الأحوال المدنية الليبية، باعتبارها إحدى أهم المؤسسات السيادية المرتبطة مباشرة بالهوية الوطنية وقواعد البيانات السكانية. وينطلق التحليل من دراسة البنية المؤسسية والتنظيمية، مرورًا بواقع إدارة الأمن السيبراني وحماية قواعد البيانات، وصولًا إلى تحليل إشكالية تسجيل المواليد دون حالة وضع باعتبارها نموذجًا تطبيقيًا يكشف حجم الخلل في الحوكمة الرقمية، وانعكاس ذلك على الأمن القومي (Al-Ali, 2021).

**المطلب الأول: واقع الحوكمة المؤسسية داخل مصلحة الأحوال المدنية**

**أولًا: الإطار الإداري والتنظيمي**

تُظهر الدراسة التحليلية لواقع مصلحة الأحوال المدنية الليبية وجود قصور هيكلي واضح في الإطار الإداري والتنظيمي الحاكم لعمل المصلحة، حيث لا تزال تعتمد بدرجة كبيرة على نماذج الإدارة التقليدية التي تركز على تسيير الأعمال اليومية، دون تبني مفهوم الحوكمة المؤسسية الحديثة القائم على التخطيط الاستراتيجي، وضوح الصلاحيات، والمساءلة، وإدارة المخاطر (Laudon & Laudon, 2020). ويُلاحظ غياب سياسات مكتوبة ومعلنة للأمن السيبراني تُحدد بشكل دقيق كيفية حماية قواعد البيانات، وآليات الاستجابة للحوادث السيبرانية، وإجراءات إدارة المخاطر الرقمية. كما تفتقر المصلحة إلى هياكل تنظيمية متخصصة تُعنى بالأمن السيبراني، مثل وحدات إدارة المخاطر الرقمية أو فرق الاستجابة للحوادث (Incident Response Teams)، وهو ما يؤدي إلى التعامل مع التهديدات الرقمية بأسلوب ردّ الفعل بدلًا من الوقاية المسبقة (Turmoil in Libya: Major Industries Hit by Massive DDoS Attacks, 2023nsfocusglobal.com). إضافة إلى ذلك، يبرز ضعف واضح في الفصل بين الصلاحيات والمسؤوليات، حيث تتداخل الأدوار الإدارية والتقنية دون وجود توصيف وظيفي دقيق، ما يخلق بيئة تنظيمية غير منضبطة تُسهّل الأخطاء الإدارية والتجاوزات الفنية. ويؤكد Osborne أن ضعف الحوكمة المؤسسية يؤدي إلى هشاشة الأداء العام للمؤسسات السيادية، خاصة في البيئات التي تعاني من عدم الاستقرار السياسي والمؤسسي، إذ تصبح المؤسسات أقل قدرة على حماية مواردها الاستراتيجية وأكثر عرضة للاختراق والانهيار الوظيفي (Libya Political Risk Report, 2026thegeopoliticaldesk.com). وفي السياق الليبي، يتضاعف أثر هذا الخلل نتيجة تعقيدات المرحلة الانتقالية، وضعف التنسيق بين الجهات الحكومية، وغياب رؤية وطنية شاملة لحوكمة التحول الرقمي (Libya Crisis Response Plan 2025 - 2026, 2025crisisresponse.iom.int).

**ثانيًا: مركزية القرار وضعف الرقابة**

تعاني مصلحة الأحوال المدنية من مركزية شديدة في اتخاذ القرار، حيث تتركز الصلاحيات في مستويات إدارية عليا دون وجود تفويض فعّال أو نظم رقابية متدرجة. وتؤدي هذه المركزية إلى بطء الاستجابة للمشكلات التشغيلية والأمنية، فضلًا عن إضعاف قدرة الوحدات الفنية على اتخاذ قرارات فورية لمعالجة المخاطر السيبرانية (Kraemer et al., 2009). كما يبرز ضعف واضح في آليات الرقابة الداخلية والتدقيق، سواء من حيث مراجعة الإجراءات أو مراقبة سلامة البيانات. ويترتب على ذلك صعوبة اكتشاف التجاوزات الإدارية أو التلاعب بالبيانات في مراحل مبكرة، وضعف المساءلة القانونية والإدارية، ما يخلق بيئة خصبة للفساد المؤسسي والتلاعب الداخلي (Libyan Prosecutors Uncover Large-Scale Identity Manipulation, 2025libyareview.com). وتشير دراسات الحوكمة المؤسسية إلى أن غياب نظم الرقابة الفعالة يُعد من أبرز مصادر الفساد الإداري، إذ يسمح بتراكم الممارسات غير القانونية دون رصد أو محاسبة (Al-Ali, 2021).

**المطلب الثاني: تحليل واقع الأمن السيبراني في قواعد البيانات**

**أولًا:إدارة الصلاحيات والوصول**

تُعد إدارة الصلاحيات والتحكم في الوصول (Access Control) أحد الأعمدة الأساسية للأمن السيبراني، خاصة في المؤسسات التي تتعامل مع بيانات سيادية حساسة. إلا أن الواقع العملي داخل مصلحة الأحوال المدنية يكشف عن اختلالات جوهرية في هذا الجانب، حيث يتم منح صلاحيات واسعة للموظفين دون ضوابط دقيقة تستند إلى مبدأ الحاجة الفعلية للعمل (Need-to-Know) (Stallings & Brown, 2018). ويُلاحظ غياب تطبيق مبدأ الحد الأدنى من الامتيازات (Principle of Least Privilege)، ما يعني أن العديد من المستخدمين يمتلكون صلاحيات تفوق متطلبات مهامهم الوظيفية، الأمر الذي يزيد من احتمالات إساءة الاستخدام أو الاختراق الداخلي. كما تعاني المصلحة من ضعف أنظمة التتبع والمراجعة الدورية لسجلات الدخول، ما يجعل من الصعب تحديد المسؤوليات في حال وقوع اختراق أو تلاعب بالبيانات (ISO, 2018).

**ثانيًا: أمن البيانات وسلامتها**

تشير المؤشرات الميدانية والتحليلية إلى ضعف تطبيق سياسات أمن البيانات داخل مصلحة الأحوال المدنية، لا سيما فيما يتعلق بضمان سلامة البيانات (Data Integrity). ويشمل هذا الضعف غياب إجراءات صارمة للتحقق من صحة المدخلات، وقصور آليات تدقيق البيانات قبل اعتمادها رسميًا، إضافة إلى ضعف حماية قواعد البيانات من التعديل غير المشروع (Schneier, 2015). ويُعد تسجيل المواليد دون حالة وضع مثالًا بارزًا على هذا الخلل، حيث يتم إدخال بيانات غير موثوقة أو غير مكتملة ضمن منظومة سيادية يُفترض أن تتمتع بأعلى مستويات الدقة والموثوقية. ويؤدي ذلك إلى تشويه السجل السكاني، وإضعاف الثقة في منظومة الهوية الوطنية ككل (Libya uncovers mass identity fraud, 2025thearabweekly.com).

**المطلب الثالث: تسجيل المواليد دون حالة وضع – تحليل أمني معمق**

**أولًا: الأسباب المؤسسية للإشكالية**

ترجع إشكالية تسجيل المواليد دون حالة وضع إلى مجموعة معقدة من العوامل المؤسسية، من أبرزها ضعف التنسيق بين الجهات الصحية ومصلحة الأحوال المدنية، وغياب الربط الإلكتروني الآمن بين المستشفيات ومنظومة التسجيل المدني، ما يفتح المجال أمام إدخال بيانات غير دقيقة أو مزورة (Public Prosecution: Forgery of 16 family records, n.d.facebook.com). كما تلعب الضغوط الاجتماعية والإنسانية دورًا في تغذية هذه الظاهرة، خاصة في ظل النزاعات المسلحة، وحالات النزوح، وفقدان الوثائق الرسمية. ويُضاف إلى ذلك استغلال بعض الأطراف للثغرات الإدارية والقانونية لتحقيق مكاسب غير مشروعة، سواء عبر تسجيل هويات وهمية أو التلاعب في البيانات الديموغرافية (Albrecht et al., 2018).

**ثانيًا: البعد السيبراني للإشكالية من منظور حوكمة الأمن السيبراني**

تُعد إشكالية تسجيل المواليد دون حالة وضع تهديدًا مركبًا، لأنها لا تمس جانبًا تقنيًا فحسب، بل تضرب في عمق سلامة قواعد البيانات السيادية، وتُضعف الثقة في منظومة الهوية الوطنية، وتفتح المجال أمام تزوير ممنهج طويل الأمد يصعب اكتشافه ومعالجته .(McConnell, 2019)

**المطلب الرابع: تقييم مستوى تطبيق حوكمة الأمن السيبراني**

بناءً على النماذج الدولية لحوكمة الأمن السيبراني، يمكن تقييم واقع مصلحة الأحوال المدنية الليبية على أنه لا يزال في مرحلة أولية جدًا من التطبيق. ويتجلى ذلك في ضعف القيادة الاستراتيجية للأمن السيبراني، وغياب إطار تشريعي داعم، وقصور واضح في إدارة المخاطر، إضافة إلى ضعف الاستثمار في العنصر البشري والتدريب المتخصص (Libyan National Information Security & Safety Authority, 2024thearabweekly.com).

**خلاصة المبحث الثالث**

خلص هذا الفصل إلى أن ضعف تطبيق حوكمة الأمن السيبراني داخل مصلحة الأحوال المدنية الليبية يُعد العامل الرئيس في تفاقم المخاطر التي تهدد الهوية الوطنية وقواعد البيانات السيادية. كما أظهر التحليل أن معالجة إشكالية تسجيل المواليد دون حالة وضع لا يمكن أن تتم بمعزل عن إصلاح مؤسسي شامل قائم على مبادئ الحوكمة، يشمل الإطار القانوني، الهيكل التنظيمي، إدارة المخاطر، وبناء القدرات البشرية، بما يضمن حماية الأمن القومي في بعده الرقمي .

**المبحث الرابع: حوكمة الأمن السيبراني كمدخل استراتيجي لحماية الهوية الوطنية الليبية وقواعد بياناتها: الحلول والمقترحات**

**المطلب الأول: حوكمة الأمن السيبراني كإطار استراتيجي شامل لمعالجة التهديدات**

**أولًا: حوكمة الأمن السيبراني من المعالجة الجزئية إلى المعالجة الشاملة**

أثبتت التجارب الدولية أن التعامل مع مخاطر الأمن السيبراني بمنطق الحلول التقنية الجزئية لا يحقق الحماية المستدامة للأصول الرقمية السيادية، ما لم يكن ذلك في إطار حوكمة شاملة تضبط السياسات، وتحدد المسؤوليات، وتربط الأمن السيبراني بالأهداف الاستراتيجية للدولة .(Calder, 2018) وتُعد حوكمة الأمن السيبراني إطارًا إداريًا وتنظيميًا يهدف إلى ضمان أن تتوافق سياسات الأمن السيبراني مع متطلبات الأمن القومي وان تدار المخاطر السيبرانية بشكل استباقي لا تفاعلي وبأن تدمج الاعتبارات القانونية والاجتماعية مع الحلول التقنية .(What is Cyber Governance? - ZenGRC, 2022zengrc.com) وفي الحالة الليبية، تبرز الحاجة إلى هذا الإطار بشكل مضاعف، نظرًا لهشاشة المؤسسات، وتعدد مراكز القرار، وضعف التنسيق بين الجهات ذات العلاقة بالهوية الوطنية (Libya Still Mired in Political Deadlock, 2025press.un.org).

**ثانيًا: متطلبات تطبيق حوكمة الأمن السيبراني في مصلحة الأحوال المدنية**

يتطلب تطبيق حوكمة الأمن السيبراني داخل مصلحة الأحوال المدنية توافر مجموعة من المرتكزات الأساسية، من أبرزها: القيادة الاستراتيجية: من خلال تبني الإدارة العليا للأمن السيبراني كأولوية وطنية. الإطار التشريعي: عبر سن قوانين واضحة تنظم حماية البيانات السيادية. الهياكل التنظيمية: بإنشاء وحدات مختصة بإدارة المخاطر السيبرانية. المساءلة والرقابة: لضمان عدم إساءة استخدام الصلاحيات. إدارة المخاطر: بالانتقال من رد الفعل إلى التخطيط الاستباقي (Understanding NIST Cybersecurity Framework (CSF) 2.0 in 2026, 2025techdemocracy.com).

**المطلب الثاني: تفعيل دور الباحث الاجتماعي في حصر المواطنين كآلية داعمة للحوكمة .**

**أولًا: البعد الاجتماعي لحماية الهوية الوطنية**

لا يمكن حماية الهوية الوطنية الرقمية بالوسائل التقنية فقط، لأن الهوية في جوهرها ليست مجرد بيانات رقمية، بل انعكاس لواقع اجتماعي وقانوني وثقافي. ومن هنا تبرز أهمية البعد الاجتماعي في معالجة الخلل الحاصل في قواعد بيانات الأحوال المدنية (Albrecht et al., 2018). ويُعد الباحث الاجتماعي أداة محورية في هذا السياق، كونه يمتلك القدرة على: قراءة الواقع الاجتماعي. التحقق من العلاقات الأسرية. فهم السياقات المحلية. كشف التناقض بين الواقع والسجلات الرسمية (Silverman, 2016).

**ثانيًا: آليات الحصر الميداني ودورها في تعزيز سلامة البيانات**

يُسهم تكليف الباحث الاجتماعي بالحصر الميداني للمواطنين من خلال الزيارات المنزلية في: التحقق من صحة واقعات الميلاد ، كشف الحالات المسجلة دون حالة وضع ، رصد حالات التزوير أو الانتحال ، تصحيح البيانات بالتنسيق مع الجهات المختصة ، ويؤدي هذا الإجراء إلى تعزيز سلامة قواعد البيانات ، وهو أحد الأركان الثلاثة للأمن السيبراني (السلامة ، السرية ، التوافر) .(Checkel, 2017)

**ثالثًا: الأثر الأمني الوطني للحصر الاجتماعي**

يتجاوز دور الباحث الاجتماعي البعد الإداري ليصل إلى البعد الأمني ، حيث يسهم الحصر الدقيق في: منع التسلل غير المشروع إلى الهوية الوطنية ، حماية التركيبة السكانية ، دعم نزاهة العمليات الانتخابية ، تعزيز الاستقرار الاجتماعي (Libya Crisis Response Plan 2025 - 2026, 2025crisisresponse.iom.int). وبذلك يصبح الباحث الاجتماعي جزءًا من منظومة الأمن القومي ، وليس مجرد موظف إداري.

**المطلب الثالث: إعادة العمل بمنظومة البصمة الوراثية (DNA) كحل سيادي**

**أولًا: منظومة DNA وأهميتها في نظم الهوية الحديثة**

تُعد البصمة الوراثية (DNA) من أكثر أدوات التحقق دقة وموثوقية، نظرًا لارتباطها بالهوية البيولوجية للفرد، واستحالة تزويرها أو التلاعب بها .(Butler, 2015) وقد أثبتت العديد من الدول أن دمج منظومة DNA في نظم الأحوال المدنية أسهم في: الحد من تزوير الهويات ، ضبط النسب ، حماية السجلات المدنية من العبث (Gill, 2014). ثانيًا: دور DNA في معالجة إشكالية تسجيل المواليد دون حالة وضع تمثل منظومة DNA حلًا جذريًا لإشكالية تسجيل المواليد دون حالة وضع، من خلال: التحقق العلمي من العلاقة البيولوجية بين المولود ووالديه ، منع تسجيل مواليد دون سند قانوني أو اجتماعي ، دعم القرارات الإدارية بأدلة علمية قاطعة (Butler, 2015). ثالثًا: الضوابط القانونية والأخلاقية لاستخدام DNA يتطلب استخدام منظومة DNA وضع ضوابط صارمة، تشمل: حماية الخصوصية ، تحديد نطاق الاستخدام ، منع إساءة استغلال البيانات البيولوجية ، إخضاع المنظومة لرقابة قضائية وتشريعية (Data protection laws in Libya, 2024dlapiperdataprotection.com).

**المطلب الرابع: المقترحات التشريعية والتقنية والمؤسسية**

تعد مصلحة الأحوال المدنية الليبية من أهم المؤسسات السيادية في الدولة، نظرًا لارتباطها المباشر بهوية المواطن وحقوقه القانونية والسياسية والاجتماعية. إلا أن هذه المصلحة تعاني من هشاشة واضحة في بنيتها التشريعية والتقنية والمؤسسية، مما يجعل قواعد بياناتها عرضة للاختراق والتلاعب، ويؤثر سلبًا على الثقة العامة وعلى الأمن الوطني. وعليه، تبرز الحاجة الملحّة إلى وضع مقترحات شاملة لمعالجة هذه الإشكاليات (Hackers attack Libya's civil registry database, 2016libyaobserver.ly).

**أولًا: المقترحات التشريعية**

إصدار قانون وطني لحماية البيانات الشخصية يحدد آليات جمع البيانات وتخزينها ومعالجتها، ويجرّم أي استخدام غير قانوني أو تسريب للمعلومات الشخصية ، تحديث القوانين المنظمة للأحوال المدنية بحيث

تتلاءم مع التحول الرقمي، وتحدد المسؤوليات القانونية في حال الاختراق أو التلاعب بالبيانات ، تشديد العقوبات على الجرائم الإلكترونية خاصة الجرائم التي تستهدف السجلات المدنية، باعتبارها تمس الأمن القومي والهوية الوطنية ، تنظيم صلاحيات الوصول إلى البيانات من خلال نصوص قانونية واضحة تمنع الاستخدام الفردي أو غير المصرّح به للأنظمة (Libya: Revoke Repressive Anti-Cybercrime Law, 2023hrw.org).

**ثانيًا: المقترحات التقنية**

تحديث البنية التحتية الرقمية عبر استخدام خوادم مؤمنة، وأنظمة تشغيل محدثة، وبرمجيات أصلية. تطبيق أنظمة الحماية السيبرانية مثل التشفير، والجدران النارية (Firewalls)، وأنظمة كشف التسلل (IDS).النسخ الاحتياطي الدوري للبيانات وتخزينه في مواقع آمنة منفصلة لتفادي فقدان المعلومات أو العبث بها ، اعتماد نظام الدخول متعدد العوامل (Multi-Factor Authentication) للحد من الاختراقات الناتجة عن سرقة كلمات المرور ، إجراء اختبارات أمنية دورية للكشف عن الثغرات ومعالجتها قبل استغلالها (Turmoil in Libya: Major Industries Hit by Massive DDoS Attacks, 2023nsfocusglobal.com).

**ثالثًا: المقترحات المؤسسية**

إعادة هيكلة مصلحة الأحوال المدنية بما يضمن الفصل بين المهام الإدارية والتقنية والرقابية ، تأهيل الكوادر البشرية من خلال التدريب المستمر في مجال أمن المعلومات والتحول الرقمي ، إنشاء وحدة متخصصة في الأمن السيبراني داخل المصلحة ، تتولى حماية الأنظمة ومراقبة أي نشاط مشبوه ، تعزيز الرقابة والمساءلة عبر لجان تفتيش داخلية وخارجية لمتابعة الأداء والالتزام بالمعايير ، التعاون مع جهات وطنية ودولية للاستفادة من الخبرات والتجارب في مجال حماية السجلات المدنية (Libyan Government Trains Personnel in Electoral Cyber Threats, 2023 darkreading.com). إن حماية قاعدة بيانات مصلحة الأحوال المدنية الليبية ليست خيارًا، بل ضرورة وطنية تفرضها متطلبات الأمن والاستقرار وبناء الدولة. ولا يمكن تحقيق ذلك إلا من خلال مقاربة متكاملة تجمع بين التشريع الصارم، والتقنية الحديثة، والإدارة المؤسسية الفعالة، بما يضمن صون هوية المواطن الليبي وحماية حقوقه (Libya trapped in a cycle of political crisis, 2025gisreportsonline.com).

**الخاتمة**

خلصت هذه الدراسة إلى أن الهوية الوطنية الليبية وقواعد بياناتها السيادية تواجه تهديدات حقيقية ومتزايدة في ظل التحول الرقمي، وضعف البنية المؤسسية، وغياب الأطر الفعالة لحوكمة الأمن السيبراني. وقد أثبت البحث أن مصلحة الأحوال المدنية تمثل خط الدفاع الأول عن الهوية الوطنية، وأن أي خلل في إدارتها أو حماية بياناتها لا ينعكس على الجانب الإداري فحسب، بل يمتد ليطال الأمن القومي الليبي بأبعاده السياسية والاجتماعية والاقتصادية (Al-Ali, 2021). وأظهرت الدراسة أن إشكالية تسجيل المواليد دون حالة وضع ليست مجرد تجاوز إداري، بل تمثل خطرًا استراتيجيًا يهدد سلامة السجل المدني، ويُسهم في تشويه التركيبة السكانية، ويقوّض الثقة في مؤسسات الدولة. كما بيّنت أن معالجة هذه الإشكالية لا يمكن أن تتم عبر حلول تقنية معزولة، بل تتطلب مقاربة شاملة قائمة على حوكمة الأمن السيبراني، تدمج بين التشريع، والتقنية، والعنصر البشري، والبعد الاجتماعي (Libya uncovers mass identity fraud, 2025thearabweekly.com). وأكدت النتائج أن تفعيل دور الباحث الاجتماعي في الحصر الميداني للمواطنين، إلى جانب إعادة العمل بمنظومة البصمة الوراثية (DNA)، يمثلان ركيزتين أساسيتين في تعزيز سلامة قواعد البيانات، وحماية الهوية الوطنية من التلاعب والتزوير، شريطة أن يتم ذلك ضمن إطار قانوني وأخلاقي واضح (Butler, 2015). وفي الختام، توصي الدراسة بضرورة الانتقال من التعامل مع الأمن السيبراني كمسألة تقنية إلى اعتباره قضية سيادية وأمنا قومياً يستوجب إرادة سياسية واصلاحا مؤسسيا واستثمارا طويل الأمد في الحوكمة بما يضمن حماية الهوية الوطنية الليبية وصون مستقبل الدولة.

**النتائج**

توصلت الدراسة من خلال التحليل النظري والواقعي إلى النتائج التالية:

1. **هشاشة منظومة الأمن السيبراني في ليبيا:** تعاني مصلحة الأحوال المدنية من ضعف بنيوي في تطبيق معايير حوكمة الأمن السيبراني، حيث تفتقر إلى استراتيجية وطنية شاملة، وتعتمد على أنظمة تقنية متقادمة تفتقد للتحديثات الأمنية اللازمة.
2. **ظاهرة "أبناء من ورق" كتهديد وجودي:** كشفت الدراسة عن خطورة ظاهرة تسجيل المواليد دون "حالة وضع" (ولادة حقيقية)، واعتبرتها تهديداً سيبرانياً غير مباشر يمس الأمن القومي، ويؤدي إلى تضخم سكاني وهمي، وهدر للمال العام، وتشويش على الاستحقاقات الانتخابية.
3. **القصور التشريعي والتنظيمي:** يوجد فجوة تشريعية واضحة تتمثل في غياب قانون خاص لحماية البيانات الشخصية وقواعد البيانات السيادية، وعدم مواكبة التشريعات الحالية (مثل قانون الأحوال المدنية) للتطورات الرقمية المتسارعة.
4. **المخاطر البشرية والإدارية:** يمثل العامل البشري الحلقة الأضعف، حيث تعاني المصلحة من سوء إدارة الصلاحيات (غياب مبدأ الحد الأدنى من الامتيازات)، وضعف التدريب، مما يسهل الاختراقات الداخلية والفساد الإداري.
5. **ارتباط الأمن السيبراني بالسيادة الوطنية:** أثبتت الدراسة أن حماية قواعد بيانات الأحوال المدنية لم تعد مسألة فنية وتقنية فحسب، بل هي ركيزة أساسية للسيادة الوطنية والاستقرار السياسي والاجتماعي للدولة.
6. **غياب التكامل بين المؤسسات:** وجود انفصال في الربط الإلكتروني الموثوق بين الجهات المولدّة للبيانات (المستشفيات) والجهة الموثقة لها (السجل المدني)، مما خلق بيئة خصبة للتزوير.

**التوصيات**

بناءً على النتائج السابقة، توصي الدراسة بالآتي:

1 **على المستوى التشريعي والقانوني:**

- **إصدار قانون شامل للأمن السيبراني وحماية البيانات:** ضرورة الإسراع في سن تشريعات تجرم التلاعب بالهوية الرقمية وتحدد عقوبات رادعة، وتنظم حماية البنى التحتية الحيوية.
- **تحديث قانون الأحوال المدنية:** تعديل النصوص القانونية لتشمل الجوانب الرقمية، وإضفاء الحجية القانونية الكاملة للسجلات الإلكترونية المحمية.

2 **على المستوى التقني والفني:**

- **الربط الإلكتروني الآمن:** إنشاء منظومة ربط إلكتروني مباشر ومشفر بين وزارة الصحة (المستشفيات) ومصلحة الأحوال المدنية لضمان عدم تسجيل أي مولود إلا بوجود إشعار ولادة إلكتروني موثق (حالة وضع حقيقية).
- **تعزيز البنية التحتية:** تحديث الخوادم والأنظمة البرمجية، وتطبيق تقنيات التشفير المتقدمة، وأنظمة كشف التسلل (IDS/IPS).
- **تنظيف قاعدة البيانات:** إجراء مراجعة فنية وتدقيق شامل لقاعدة البيانات الحالية لتنقيتها من القيود الوهمية (أبناء من ورق) باستخدام تقنيات الذكاء الاصطناعي وتحليل البيانات.

3 **على المستوى الإداري والحوكمة:**

- **تطبيق إطار حوكمة معتمد:** تبني إطار عمل عالمي (مثل NIST أو ISO 27001) لإدارة مخاطر الأمن السيبراني داخل المصلحة.
- **إدارة الصلاحيات بصرامة:** تطبيق سياسة "الحد الأدنى من الصلاحيات" (Least Privilege)، وفصل المهام (Segregation of Duties) لمنع انفراد موظف واحد بالقدرة على الإضافة أو التعديل الجوهري.
- **تأسيس وحدة للأمن السيبراني:** إنشاء إدارة متخصصة تتبع أعلى هرم إداري في المصلحة، تعنى بالمراقبة المستمرة والاستجابة للحوادث السيبرانية.
-

4 **على المستوى البشري والتوعوي:**

- **بناء القدرات:** عقد دورات تدريبية مكثفة للموظفين حول الأمن الرقمي وكيفية التعامل مع البيانات الحساسة.
- **تعزيز الرقابة والمساءلة:** تفعيل آليات الرقابة الداخلية والتدقيق المستمر على مدخلات النظام، ومحاسبة المتورطين في عمليات التزوير السابقة.

**Compliance with ethical standards**

*Disclosure of conflict of interest*

The author(s) declare that they have no conflict of interest.

**المراجع:**

**المراجع العربية**


- الزاوي، ح. (2016). الهوية الوطنية وأثرها في بناء الدولة الليبية [National identity and its impact on building the Libyan state]. دار الجامعة الجديدة.
- العرفي، أ. (2019). الأحوال المدنية والسيادة الوطنية في ليبيا [Civil status and national sovereignty in Libya]. دار الفكر الجامعي.
- المرغني، س. (2020). التحديات القانونية للأحوال المدنية الليبية [Legal challenges for Libyan civil status]. دار النهضة العربية.
- مجيد، ص. ص. (2022). الأمن السيبراني وأثره في قوة الدولة [Cybersecurity and its impact on state power]. مجلة العلوم التربوية والإنسانية، 18، 174–201.
- على قاسمي /هاشم كاظم(2025). تأثير الهجمات السيبرانية على الحقوق المدنية والرقمية [Impact of cyber attacks on civil and digital rights]. مجلة الجامعة العراقية، 72(5)، 128.
- عبد الجبار الرفاعي. (2025). الهوية في شراك الإيديولوجيا [Identity in the ideology trap]. مركز دراسات فلسفة الدين.


**المراجع الاجنبية**


- **Al-Ali, Z. (2021).** *Cybersecurity challenges in transitional states: The Libyan experience*. Springer.
- **Albrecht, C., et al. (2018).** *Social dimensions of cybersecurity governance*. Springer.
- **Anderson, J. (2016).** *Digital security and national identity*. Cambridge University Press.
- **Behl, A., & Behl, A. (2017).** *Cyber security management: A strategic approach*. Routledge.
- **Butler, J. M. (2015).** *Forensic DNA typing: Biology, technology, and genetics of STR markers*. Elsevier.
- **Calder, A. (2018).** *IT governance and cybersecurity: A practical guide*. IT Governance Publishing.
- **Checkel, J. (2017).** *Social verification in transitional governance*. Cambridge University Press.
- **Cordesman, A. (2019).** *Cybersecurity and national defense: Global perspectives*. CSIS Press.
- **Elaswad, A., & Jensen, C. D. (2016).** *Identity management for e-government: Libya as a case study*. IEEE Xplore.
- **European Union Agency for Cybersecurity (ENISA). (2024).** *2024 report on the state of cybersecurity in the Union*.
- **Gibson Dunn. (2024).** *U.S. cybersecurity and data privacy outlook and review – 2024*.
- **Heeks, R. (2017).** *Information and communication technology for development*. Routledge.
- **International Telecommunication Union (ITU). (2024).** *Global cybersecurity index 2024*. ITU Publications.
- **ISO. (2018).** *ISO/IEC 27001: Information security management systems*. ISO Publications.
- **Laudon, K. C., & Laudon, J. P. (2020).** *Management information systems: Managing the digital firm* (16th ed.). Pearson.
- **McConnell, S. (2019).** *Cybersecurity for business and government*. O'Reilly Media.
- **Schneier, B. (2015).** *Data and Goliath: The hidden battles to collect your data and control your world*. Wiley.
- **Silverman, D. (2016).** *Qualitative research* (4th ed.). Sage Publications.
- **Stallings, W., & Brown, L. (2018).** *Computer security: Principles and practice* (4th ed.). Pearson.
- **Turban, E., Pollard, C., & Wood, G. (2018).** *Information technology for management: Digital strategies for insight, action, and sustainable performance* (10th ed.). Pearson.
- **U.S. Department of Justice. (2024).** *National security division: Provisions regarding access to Americans' bulk sensitive personal data*. Federal Register.
- **World Economic Forum. (2020).** *The global risks report 2020*. WEF Publications.