وزارة التعليم العالي والبحث العلمي
جامعة عمار ثليجي بالأغواط
كلية الحقوق

الموضوع:

الامن المعلوماتي ودوره في تكريس مكافحة الفساد

مذكرة مقدمة لنيل شهادة ماستر حقوق

تخصص: قانون جنائي وعلوم جنائية

من اعداد :

- مكنزية باية
- بن دومة كريمة

اشراف الأستاذ:

أ. د. قريبيز مراد

لجنة المناقشة

الاسم و اللقب	الدرجة العلمية	الصفة
تركي محمد سعيد	أستاذ محاضر أ	رئيسا
قريبيز مراد	أستاذ التعليم العالي	مشرفا
غريبي علي	أستاذ محاضر أ	مناقشا

السنة الجامعية: 2024- 2025

شكر وعرفان

حمد الله تعالى ونشكره الذي سدد خطانا ووفقنا في هذا العمل المتواضع

يسرنا أن نتقدم بالشكر والامتنان الذي قبل الاشراف على هذا العمل ولم يبخل علينا بنصائحه وارشاداته نتمنى له دوام الصحة والعافية والمزيد من النجاح والتألق في حياته

"" قريبيز مراد ""

والى كل أساتذتنا بالكلية الذين رافقونا طيلة مشوارنا الدراسي

الى كل من ساعدنا وتحمل معنا مشاق العمل والتعب من قريب وبعيد

مقدمة

مقدمة

لقد أضحى الفساد اليوم بجميع صوره وأشكاله من أبرز التحديات التي تواجه الأنظمة القانونية والسياسية والاقتصادية في مختلف دول العالم دون تمييز يذكر سواء المتقدمة منها أو النامية. ويعد نوع الفساد الإداري والمالي آفة مدمّرة تمسّ بعمق مبدأ سيادة القانون، وتقوّض جهود التنمية المستدامة، وتزعزع الثقة في مؤسسات الدولة.

لقد شهد مفهوم الفساد في العقود الأخيرة تحوّلًا نوعيًا بفعل التطورات التكنولوجية التي أعادت تشكيل المشهد الإداري والاقتصادي والسياسي في مختلف دول العالم. ففي الوقت الذي ساهمت فيه الرقمنة في تحسين كفاءة الأداء، وتسهيل الوصول إلى المعلومات، وتقليص البيروقراطية، إلا أنها أفرزت بالمقابل أشكالًا جديدة ومعقدة من الفساد يصعب تتبّعها أو إثباتها بالطرق التقليدية.

فلم يعد الفساد في شكله التقليدي الذي يقتصر على الرشوة المباشرة أو إساءة استعمال النفوذ في المكاتب الإدارية، بل أصبح يتخذ صورًا رقمية متقدمة، منها التلاعب في قواعد البيانات العمومية، تعديل الوثائق الإلكترونية، اختراق الأنظمة المالية، أو حذف الأدلة الرقمية التي تدين المتورطين في قضايا فساد .وقد يؤدي ذلك إلى طمس الحقائق أو تعطيل عمل الجهات الرقابية والقضائية، مما يزيد من صعوبة الكشف عن مرتكبي الفساد.

ويعد هذا النوع من الفساد أكثر خطورة، لأنه يستغل ضعف البنية المعلوماتية وغياب نظم الحماية الرقمية، كما يستفيد من المهارات التقنية المتقدمة لبعض الفاعلين المتورطين في الفساد، سواء داخل المؤسسات أو خارجها.

وفي ظل هذا التحدي العالمي ظهرت الحاجة إلى تطوير آليات فعالة للوقاية والمكافحة لا سيما في العصر الرقمي الذي يشهد توسعًا كبيرًا في استخدام تكنولوجيا المعلومات والاتصال.

وفي هذا السياق برز "الأمن المعلوماتي "كأحد المفاهيم الحديثة التي تكتسي أهمية قانونية متزايدة، لِما له من دور محوري في حماية البيانات، والحفاظ على سرية الوثائق

وضمان سلامة المعاملات الرقمية، ومنع اختراق الأنظمة التي قد تُستخدم في التلاعب أو إخفاء جرائم الفساد، فقد أصبحت الحكومات تعتمد بشكل كبير على النظم الإلكترونية في تسيير مختلف القطاعات، مما يفرض ضرورة مواكبة التطور الرقمي بمنظومة قانونية وأمنية متكاملة قادرة على التصدي لمخاطر الفساد الإلكتروني والمعلوماتي.

فالأمن المعلوماتي لا ينحصر في الحماية التقنية للأنظمة والشبكات، بل يمتد إلى مستوى تأمين المعاملات، حماية البيانات الحساسة، ومنع التلاعب بالمعلومات أو التستر على الفساد من خلال الاختراقات أو الإتلاف الرقمي للوثائق .وتبرز الحاجة الملحة إلى تكامل بين الإجراءات التقنية والضوابط القانونية، بما يضمن معالجة متكاملة لظاهرة الفساد في بيئة رقمية آخذة في التوسع.

وقد أدركت الجزائر، في ظل التحولات التكنولوجية الراهنة، ضرورة تعزيز بنيتها القانونية والمؤسسية لمواجهة الجرائم الرقمية ذات الصلة بالفساد، إذ أصدر المشرع الجزائري عدة قوانين وتنظيمات ذات صلة مباشرة بموضوع الأمن المعلوماتي ومكافحة الفساد.

فعلى صعيد مكافحة الفساد، يعتبر القانون رقم 06-01 المؤرخ في 20 فبراير 2006 والمتعلق بمكافحة الفساد، الإطار المرجعي الأساسي، حيث ينص في مادته الثانية على أن:

"يُقصد بالفساد في هذا القانون كل عمل يتضمن إساءة استغلال السلطة أو الوظيفة العامة من أجل تحقيق منافع شخصية غير مشروعة، سواء بشكل مباشر أو غير مباشر."

ويشمل هذا القانون أشكالًا متعددة من الجرائم التي قد تقع في البيئة الرقمية مثل: اختلاس الأموال العامة، استغلال النفوذ، الرشوة، تبييض الأموال، وغيرها.

أما في مجال الأمن المعلوماتي، فقد تم تقنين ذلك في قانون العقوبات الجزائري المعدل بالأمر رقم 21-09 المؤرخ في 8 يونيو 2021، الذي أُدرجت فيه جرائم المعلوماتية ضمن مواده، خاصة من المادة 394 مكرر إلى المادة 394 مكرر 8، حيث يُعاقب القانون على جرائم متنوعة

هنا يظهر دور الأمن المعلوماتي كخط دفاع أساسي، ليس فقط لحماية البيانات، بل لكشف الفساد الرقمي وتوثيقه قبل طمسه أو اختراقه.

وتكمن أهمية الموضوع في تسليط الضوء على دور الأمن المعلوماتي كآلية وقائية وردعية في الحد من الفساد. ومن ثم بيان العلاقة بين تطوير البنية الرقمية وتعزيز الشفافية داخل المؤسسات. كما هو الحال الى توضيح الفجوة القانونية في التشريعات المتعلقة بحماية نظم المعلومات من الاستغلال في الفساد. وفي الأخير المساهمة في إثراء المكتبة القانونية الوطنية والعربية بدراسة تجمع بين البعد القانوني والتكنولوجي في موضوع مكافحة الفساد.

وعن اهداف الموضوع فتهدف هذه الدراسة إلى تعريف الأمن المعلوماتي وبيان عناصره القانونية والتقنية. وإبراز أشكال الفساد التي تتصل بسوء استغلال تكنولوجيا المعلومات، ومحاولة تحليل أوجه العلاقة بين الأمن المعلوماتي وفعالية آليات مكافحة الفساد. ودراسة الإطار القانوني والتنظيمي للأمن المعلوماتي في مواجهة الفساد، محليًا ودوليًا. وفي الأخير تقديم مقترحات عملية لتعزيز دور الأمن المعلوماتي في مكافحة الفساد من خلال السياسات والتشريعات.

ومن خلال كل ام سبق نطرح إشكالية الدراسة التالية في التساؤل التالي

إلى أي مدى يمكن اعتبار الأمن المعلوماتي وسيلة فعالة في مكافحة الفساد؟

تعتمد الدراسة على **المنهج الوصفي التحليلي** من خلال توصيف المفاهيم وتحليل النصوص القانونية ذات الصلة بالأمن المعلوماتي والفساد، بالإضافة إلى **المنهج المقارن** عند الحاجة لمقارنة التجارب الدولية الرائدة بالتجربة الوطنية (الجزائرية أو حسب الدولة محل الدراسة).

وقد قسمنا الدراسة الى الخطة التالية :

وللإجابة على الإشكالية المطروحة، ارتأينا تقسيم الموضوع إلى فصلين أساسيين:

الفصل الأول: الإطار النظري والقانوني للأمن المعلوماتي ومفهوم الفساد

الفصل الثاني: دور الأمن المعلوماتي في مكافحة الفساد

الفصل الأول: الإطار النظري والقانوني للأمن المعلوماتي ومفهوم الفساد

الفصل الأول: الإطار النظري للأمن المعلوماتي ومفهوم الفساد

تمهيد

مع تطور المجتمعات نحو الرقمنة وتنامي الاعتماد على تكنولوجيا المعلومات والاتصال في مختلف القطاعات، برزت تحديات جديدة تهدد سلامة المنظومات الرقمية، كان من أبرزها ما يتعلق بتهديدات أمن المعلومات، وتفاقم مظاهر الفساد المستحدثة في البيئة الإلكترونية. فقد غدت المعلومات، في العصر الرقمي، مورداً استراتيجياً لا يقل أهمية عن الموارد المادية والمالية، الأمر الذي فرض على الدول والمؤسسات البحث عن آليات فعّالة لحمايتها من الاستغلال غير المشروع، أو التلاعب، أو التدمير.

وفي هذا الإطار، بات من الضروري التطرق إلى البعد النظري الذي يؤسس لفهم متكامل لمفاهيم الأمن المعلوماتي والفساد، خاصة في ظل التداخل الواضح بين المعطى التكنولوجي والمعطى الإداري والقانوني. فالأمن المعلوماتي لم يعد مقتصرًا على البنية التقنية بل تحول إلى منظومة متكاملة تشمل أبعادًا بشرية، تنظيمية، وسلوكية. وبالمثل، لم يعد الفساد محصورًا في ممارسات تقليدية، بل تطور ليأخذ أشكالًا جديدة داخل البيئات الرقمية، منها العبث بالبيانات، تسريب المعلومات، واستغلال الثغرات السيبرانية لأغراض غير مشروعة.

وعليه، يهدف هذا الفصل جاء وفقا للتالي:

المبحث الأول: الإطار المفاهيمي للأمن المعلوماتي

المبحث الثاني: الفساد ومظاهره في المجال المعلوماتي

المبحث الأول: الإطار المفاهيمي للأمن المعلوماتي

مع تزايد الاعتماد على النظم الرقمية في تسيير مختلف شؤون المؤسسات الحكومية والخاصة، أضحى الحفاظ على أمن المعلومات يشكل أحد المرتكزات الأساسية لضمان استمرارية العمل وحماية المصالح الحيوية للدول والمجتمعات. ولم يعد الأمن المعلوماتي مجرد إجراء تقني يُتخذ لحماية الأجهزة والبرمجيات، بل أصبح منظومة متكاملة تشمل السياسات، والضوابط، والبنى التنظيمية، والعناصر البشرية، الهادفة إلى تأمين البيانات والمعلومات من كل تهديد محتمل، سواء كان مصدره بشرياً أو تقنياً.

وسيتناول هذا المبحث الوقوف على المفاهيم الأساسية للأمن المعلوماتي، من خلال **(المطلب الأول)** تعريف الأمن المعلوماتي ومكوناته اما **(المطلب الثاني)** التهديدات التي تواجه أمن المعلومات في البيئة الرقمية

المطلب الأول: تعريف الأمن المعلوماتي ومكوناته

يُعد الأمن المعلوماتي من المفاهيم الحديثة التي فرضتها التطورات المتسارعة في ميدان تكنولوجيا المعلومات والاتصال، وهو مفهوم مركزي في عصر تتزايد فيه التحديات المتعلقة بحماية البيانات وتأمين الفضاء الرقمي. فقد أصبحت المعلومات موردًا استراتيجيًا حيويًا لا يقل أهمية عن باقي الموارد المادية، ما جعل تأمينها ضرورة ملحة في ظل تنامي الجرائم الإلكترونية، وتسريب الوثائق الحساسة، والاختراقات المتكررة للأنظمة.

وعليه، يهدف هذا المطلب إلى تحديد المفهوم الدقيق للأمن المعلوماتي وفقًا لما ورد في المعايير الدولية والأطر الأكاديمية **(الفرع الأول)** ثم إبراز أبرز مكوناته التي ترتكز عليها أي منظومة معلوماتية فعالة وآمنة، تمهيدًا لفهم دوره العملي في التصدي للفساد ومختلف صور التهديد المعلوماتي. **(الفرع الثاني)**

الفرع الأول " تعريف الأمن المعلوماتي

أولا: التعريف اللغوي والاصطلاحي

اختلف الباحثون والدارسون لهذا المجال على وضع تعريف موحد لأمن المعلومات فمنهم من عرفه من زاوية أكاديمية، ومنهم من عرفه من زاوية تقنية ويمكن إجمال هذه التعريفات فيما يلي:

يُشتق مصطلح "الأمن" من الطمأنينة وعدم الخوف، ويقصد به الاطمئنان إلى حماية شيء ما من التهديد. أما "المعلوماتي"، فهو نسبة إلى المعلومات الرقمية أو الإلكترونية. وعليه، فإن الأمن المعلوماتي هو الحماية من أي تهديد يمس هذه المعلومات.

عرف فلاديمير قوان Vladimir Gnuan) امن المعلومات على أنه: "جميع الوسائل التي يتم توفيرها للحد من ضعف نظام المعلومات، ضد مختلف التهديدات سوءا المفاجئة أو المتعمدة. وبعبارة أخرى هي مجموع التقنيات التي تضمن الموارد نظام المعلومات سوءا (الأجهزة أو البرامج الاستخدام الأمثل وفي السياق المحدد".

وبصفة عامة فان منهجية أمن المعلومات تقوم على ثلاثة عناصر مهمة كالاتي:

– إجراء تحليل للمخاطر (Effectuer une analyse des risques): وذلك لأنه من غير الممكن حماية أصول المؤسسة من المخاطر التي لست على علم بها، ويتم ذلك عن طريق قياس احتمال حصولها والآثار المحتملة الناجمة عنها.[1]

– وضع سياسة أمنية ويتم ذلك مباشرة بعد إجراء فحص أو تحليل للمخاطر ويكون الهدف من هذه السياسة هو:

- تحديد إطار استخدام موارد المعلومات.
- تحديد التقنيات الأمنية التي سيتم توفيرها في مختلف مصالح المؤسسة.
- توعية الموظفين والمستخدمين حول أهمية امن المعلومات.

[1] Vladimir aman Gnuan, Concevoir la sécurité informatique en entreprise, 2014, p 13… 15.

– تنفيذ التقنيات الأمنية هذه التقنيات هدفها هو تلبية المتطلبات الأساسية لسلامة تكنولوجيا المعلومات داخل المؤسسة. !

ويعرف ادام شوستاك (Adam Shostack) أمن المعلومات على انه: "التأكد من أن نظم المعلومات يمكن أن تعمل بالشكل المطلوب وعلى النحو المقصود في بيئة معادية. "[2]

وعرفه فارمان (Warman A.R) على انه "مجموعة من الإجراءات والتدابير الوقائية والتي تستخدم سوءا في المجال التقني أو الوقائي بهدف الحفاظ على المعلومات الأجهزة والبرمجيات، فصلا عن الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال".

ويرى دومين (Doomun) ان الامن هو ذات أهمية قصوى اذ ينبغي على المنظمة خدمة العديد من المنافسين والمستهلكين المباشرين ولذا ينبغي الحفاظ على السرية التامة للمعلومات المرسلة إليهم. [3]

وفيما يلي جملة التعريفات حول أمن المعلومات:

"هو العلم المختص بتامين المعلومات المتداولة عبر الشبكة من المخاطر التي تهددها، وهو كذلك العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تحددها، أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية والخارجية. "[4]

---

[2] Adam Shostack, "the evolution of information security", the next wave, vol 19, N° 2, 2012, p8.

[3] ندى إسماعيل جبوري، حماية امن انظمة المعلومات دراسة حالة مصرف الرافدين"، مجلة تكريت للعلوم الإدارية الاقتصادية، مجلد رقم 7، العدد 2، بغداد، 2011، ص67

[4] عبد الرحمان شعبان عطيات أمن الوثائق والمعلومات، ط 1، الرياض جامعة نايف العربية للعلوم الأمنية، 2003، ص 122

هو مجموعة الإجراءات والضوابط والقواعد والتشريعات التي توضع للحفاظ على سلامة وتكامل نظام المعلومات من التخريب والعبث والفقدان، وكذلك من التغيير والاستعمال الغير المصرح به سوءا كان هذا التغيير او التخريب مقصودا ام غير مقصود. "

عرفت المنظمة الدولية للمعايير:(2013) ISO/IEC "الأمن المعلوماتي هو حماية المعلومات من مجموعة واسعة من التهديدات لضمان استمرارية الأعمال، وتقليل الأضرار، وتعظيم عائد الاستثمار."

أما في تعريف المعهد الوطني للمعايير والتكنولوجيا:(2018) NIST فالامن المعلوماتي "هو حماية نظم المعلومات والمعلومات من الوصول غير المشروع أو التعديل أو الإتلاف أو الاستخدام أو الكشف، باستخدام وسائل إدارية وتقنية مناسبة[5]."

الأمن المعلوماتي يشمل كل الأنظمة والإجراءات التي تضمن سرية المعلومات، وصحتها، وتوافرها للمستخدمين المصرح لهم فقط.

وتعرف هيئه الاتصالات وتقنيه المعلومات السعودية امن المعلومات بانه إبقاء معلوماتك تحت سيطرتك المباشرة وعدم امكانيه الوصول اليها من طرف شخص أخر دون اذنك وأن تكون على علم بالمخاطر المترتبة عند السماح الشخص ما بالوصول الى معلوماتك الخاصة.[6]

ويعرف امن المعلومات كذلك على انه: "حماية المعلومات ونظام المعلومات من الاستخدام أو الوصول الغير المصرح، أو الكشف والتعطيل أو التدمير والتعديل، ووفقا للقانون الأمريكي فان أمن المعلومات هو السعي الحماية البيانات الخاصة بك مهما كانت حساسيتها من هؤلاء الذين يريدون إساءة استخدامها".

وهو كذلك الأساليب والوسائل المعتمدة، للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من النسخ، السرقة او التعديل أو الابتزاز أو التلف أو الضياع أو حتى التزوير

[5] رابح محمد، الجرائم المعلوماتية وأمن النظم الإلكترونية، دار الهدى للنشر والتوزيع، مصر، 2021، ص 68.

[6] Jason Andress, the basics of information security, 2nd Ed, 2014, Usa, p3.

والاستخدام الغير قانوني، فهو الإحساس الفعلي بعدم وجود إي تهديد للبنية المعلوماتية، وتجهيز البدائل لمجابهة إي تهديد حقيقي. "

وكتعريف شخصي يمكن القول بان امن المعلومات هو :

–من الناحية الأكاديمية: هو العلم الذي يبحث في نظريات واستراتيجيات وتقنيات توفير الحماية للمعلومات من مخاطر الاعتداء عليها.

–أما من الناحية التقنية هي الوسائل والإجراءات الواجب توفرها لضمان حماية المعلومات من مختلف التهديدات المتوقعة.

–ومن الناحية القانونية فهي جميع القوانين والتشريعات سواء سوءا كانت وطنية أو دولية التي تهدف إلى مكافحة الجرائم المرتكبة ضد المعلومات ونظمها ومن تم معاقبة مرتكبي هذه الجرائم.

الفرع الثاني: مكونات الأمن المعلوماتي

أولا" المكون البشري

يُعد العنصر البشري هو الحلقة الأضعف في منظومة الأمن المعلوماتي، إذ أن الجهل أو الإهمال أو حتى النية السيئة من طرف الأفراد قد تؤدي إلى اختراق النظام. لذا فالتدريب والتوعية الأمنية أمران ضروريان.

ثانيا :المكون التكنولوجي

تشكل الوسائل التقنية العمود الفقري في منظومة الأمن المعلوماتي، حيث تُمكّن من التصدي للتهديدات السيبرانية والهجمات الإلكترونية، من خلال أدوات متخصصة مصممة للكشف عن الخروقات أو منعها أو معالجتها فور وقوعها. وتُستخدم هذه الأدوات مجتمعة أو متكاملة ضمن بيئة عمل رقمية لتحقيق أقصى قدر من الحماية. من أبرز هذه الوسائل[7]." :

[7] رابح محمد، المرجع السبق، ص 72.

1- **الجدران النارية(Firewalls) :**

تعد الجدران النارية خط الدفاع الأول في أي شبكة معلوماتية، حيث تعمل كحاجز أمني بين الشبكة الداخلية الموثوقة والشبكات الخارجية غير الموثوقة (مثل الإنترنت).حيث وظيفتها الأساسية هي تصفية حركة المرور الشبكية ومنع الحزم غير المصرح بها من الدخول أو الخروج، بناءً على قواعد مُعدّة مسبقًا وتستخدم المؤسسات غالبًا الاثنين معًا لتعزيز الأمان.

2- **أنظمة كشف التسلل ومنعه**

تهدف أنظمة كشف التسلل ومنعه إلى مراقبة حركة الشبكة ورصد السلوكيات غير الطبيعية التي قد تحدث والتي قد تشير إلى محاولة اختراق لمجموعة البيانات والمعلومات التي يحتفظ بها في الأجهزة الالية وهناك نظام كشف التسلل (IDS) هذا النوع يقوم بالتنبيه إلى وجود تهديد دون التدخل، أما نظام منع التسلل (IPS) فهو يتدخل تلقائيًا لصد الهجوم، كمنع الاتصال المشبوه أو عزل النظام المصاب، في ذات السياق تعتمد هذه الأنظمة على قواعد بيانات للتهديدات المعروفة، كما قد تستعمل تقنيات الذكاء الاصطناعي لرصد الأنماط الجديدة.

3- **برامج مكافحة الفيروسات والبرمجيات الخبيثة-Anti) (Anti-Virus / Malware)**

تُستخدم هذه البرامج لاكتشاف الفيروسات، وأحصنة طروادة، وبرمجيات الفدية، وغيرها من التهديدات الرقمية التي تؤثر على البيانات ومن ثم يكون العمل على عزلها أو حذفها من النظام، كما أنه تُحدث هذه البرامج قواعد بياناتها باستمرار لمواكبة التهديدات الحديثة، وهي ضرورية على كل جهاز ونقطة اتصال، سواء في المؤسسات أو لدى المستخدمين الأفراد.

4- التشفير(Encryption)

يعد نظام التشفير أحد أهم تقنيات حماية البيانات والمعلومات، حيث يعمل على تحويل المعلومات الحساسة إلى صيغ غير مفهومة لا يمكن قراءتها إلا باستخدام مفتاح فك التشفير ويستخدم التشفير في البريد الإلكتروني، الاتصالات، قواعد البيانات، والتخزين السحابي.

5- أدوات المصادقة والتحقق من الهوية(Authentication Tools)

تهدف هذه الأدوات إلى التحقق من هوية المستخدمين قبل السماح لهم بالوصول إلى الأنظمة أو البيانات. وتشمل غالبا كلمات المرور الآمنة والمركبة والمصادقة الثنائية أو المتعددة العوامل كما هو الحال الى البطاقات الذكية أو التحقق البيومتري (بصمة الإصبع/الوجه).

وتُعد هذه الأدوات ضرورية لتقليل احتمالية التسلل الناتج عن سرقة الهوية أو استغلال الحسابات الضعيفة[8].

إن استخدام الوسائل التقنية المذكورة أعلاه بشكل متكامل لا يُمثل فقط آلية للحماية، بل يُعد إستراتيجية وقائية واستباقية ضرورية في كل مؤسسة رقمية. ويجب أن تترافق هذه الأدوات مع تحديثات منتظمة، وسياسات أمنية واضحة، وتدريب للعاملين لضمان فعاليتها.

المطلب الثاني: تهديدات الامن المعلوماتي في البيئة الرقمية

مع التزايد المستمر للتعقيد التقني والمصاعب القانونية وتوقعات حماية الخصوصية ارتفعت تحديات أمن المعلومات بشكل متسارع خلال السنوات الماضية إذ أن الانتشار الكبير لاستعمال التطبيقات القابلة للعمل مع شبكة الانترنت (Web Enabled) في تسعينيات القرن الماضي وتزايد حصة هذا الاستثمار في سوق الأسهم غالبا ما دفع بمرتبة عمليات أمن المعلومات إلى مستوى الأفضلية[9].

---

[8] خليف فوزي، أمن المعلومات في البيئة الرقمية، دار الكتب العلمية، الجزائر، 2022، ص 90.

[9] لورنس م. أوليفا، ترجمة محمد مراياتي امن تقنية المعلومات نصائح من خبراء المنظمة العربية المترجمة، ص 25-26

وتشمل التحديات التي تواجهها إدارات تقنيات امن المعلومات ما يلي:

- عدم الفهم والخلط أحيانا بين العديد من تقنيات أمن المعلومات المختلفة والمتضاربة.
- معرف من يمكن له ومن لا يمكن له الوصول للمعلومات، والأنظمة والشبكات فأحيانا قد لا تبلغ سجلات الموظفين الدقيقة بسرعة إلى إدارة تقنية المعلومات.
- عدم وجود معايير شاملة ومتفق عليها للأمن المعلوماتي.
- تحديد مستوى الصلاحيات الصحيح لكل موظف وكل مستخدم للنظام لكي يقومون بإعمالهم من دون السماح للجميع بالنفاد الكامل الجميع الملفات والأنظمة.
- معرفة من يمكن أن تثق فيهم من الموردين والشركاء والزبائن من أجل التزويد بالمعلومات فليست كل المعلومات سواء فقد تحتوي مرفقات البريد الالكتروني على فيروسات أو رسائل صور أو نصوص أو حتى تسجيلات صوتية مخفية بتقنية
- جلب مؤهلين وأخصائيين وخبراء في امن المعلومات.
- المحافظة على مقدرة هندسية للاستجابة السريعة ضد مختلف التهديدات والهجمات من الإفراد الذين يحاولون الوصول إلى معلومات قيمة.
- ضف إلى ذلك التحديات القانونية والتشريعية خاصة في دول العالم الثالث فأغلبية هذه الدول تفتقر الإطار القانوني والتشريعي لردع مرتكبي الجرائم المعلوماتية.

المبحث الثاني: الفساد ومظاهره في المجال المعلوماتي

يُعد الفساد من الظواهر الاجتماعية والسياسية والاقتصادية الأكثر خطورة على استقرار الدول ونزاهة مؤسساتها. وقد اتخذت هذه الظاهرة أبعادًا جديدة في العصر الرقمي، حيث لم تعد الممارسات الفاسدة حكرًا على التعاملات الورقية أو العلاقات الشخصية، بل تسللت إلى البيئة المعلوماتية التي باتت تمثل مسرحًا مفتوحًا لمظاهر متعددة من التلاعب والانحرافات السلوكية، مستفيدة من تطور التكنولوجيا وغياب أو ضعف آليات الرقابة الرقمية.

وقد ساهم الانتقال إلى الأنظمة المعلوماتية في كشف العديد من أشكال الفساد من جهة، لكنه في الوقت ذاته فتح المجال أمام أنماط فساد مستحدثة من جهة أخرى. لذا فإن فهم طبيعة الفساد في المجال المعلوماتي يقتضي التطرق إلى مفهوم الفساد نفسه (المطلب الأول) ، ثم تحليل أبرز مظاهره وخصائصه في البيئات الرقمية والإدارية المرتبطة بتكنولوجيا المعلومات (المطلب الثاني)

المطلب الأول: مفهوم الفساد

الفرع الأول: تعريف الفساد

أولا: التعريف اللغوي للفساد:

الفاء والسين والدال كلمة واحدة يقال : فسد الشيء يفسد فسادا وهو فاسد وفسيد. وفسد الشيء بمعنى خروجه عن موضعه أو عدم اعتداله، وبطلانه، فكلمة الفساد في اللغة ضدها الصلاح. كما جاء في قول ابن منظور في لسان العرب:" الفساد نقيض الصلاح، فسد، يفسد، فسادا، فسودا، وتفاسد القوم : تدابروا وقطعوا الأرحام واستفسد السلطان قائده إذا أساد

إيه استعصى عليه والمفسدة خلاف المصلحة، والاستفساد خلاف الاستصلاح وقالوا هذا الأمر مفسدة لكذا أي فيه فساد .[10]

فمصطلح الفساد من ناحية اللغوية لقى اهتمام من قبل الشعراء والمختصين في اللغة العربية من بينهم:

قول الراغب الأصفهاني الفساد خروج الشيء عن الاعتدال سواء كان الخروج عليه قليلا أو كثيرا وكل اعتداء في الدين أو العقل أو المال أو العارض أو النفس فهو اعتداء.[11]

وقال الشاعر أبو العتاهية : أن الشباب والفراغ والجدة مفسدة للعقل أي مفسدة والمستمع لاستخدامات العرب لهذه اللفظة يجد أنها تطلق على التلف والعطب وللاضطراب والخلل والجرب والقحط يقال فسد اللحم أو اللبن أي أنه عطب وفسد، الرجل جاوز الصواب والحكمة وفسدت الأمور اضطربت وأدركها الخلل.[12]

ثانيا : التعريف الاصطلاحي للفساد:

لقد تعددت معاني الفساد من الناحية الاصطلاحية بين مختلف الفقهاء وكذا التشريعات نظرا لأخذه العديد من المضامين المختلفة سواء في طابعها أو نظرتها وفلسفتها فالبعض يرجع ارتباطه بالبعد الحضاري من قيد وتقاليد والبعض الآخر يعتمد على أحادية النظرة التي تجعل الفساد نتيجة التسبب إداريا أو الفوضى أو استجابة للحاجة والعامل النفسي.

غير أن العامل المشترك بين تعريفات الفقهاء هو أن الفساد ظاهرة مستعصية ومعقدة تمس القطاع العام والخاص للدول وتعود عليه بالآثار الوخيمة من التطور والشفافية والنزاهة.

---

[10]– حاجة عبد العالي، أطروحة دكتوراه حقوق تخصص قانون عام للطالب تحت عنوان الآليات القانونية لمكافحة الفساد الإداري في الجزائر" ، جامعة محمد خيضر بسكرة قسم حقوق السنة الجامعية، 2012/2013ص12.

[11]– ليلى علي أحمد الشعري، المجلد الثامن من العدد الثالث والثلاثين لجولية كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية من إعداد الدكتور أستاذ مساعد بجامعة الطائف تحت عنوان السفاد مكافحته والوقاية منه (رؤية شرعية) ص 285.

[12]– حاجة عبد العالي، مرجع سابق، ص12.

1- الفساد من ناحية فقهاء علم القانون وعلم الاجتماع والقانون الإداري :

عرف فقهاء القانون ظاهرة الفساد بالعديد من التعريفات لعل من بينها :" تصرف وسلوك وظيفي سيء فاسد خلاف الاصطلاح، هدفه الانحراف وكسب الحرام، والخروج على النظام لمصلحة شخصية.[13]

- كما جاء تعريف الفساد حسب فقهاء القانون الإداري فإنه: "النشاطات التي تتم داخل الجهاز الإداري الحكومي، والتي تؤدي فعلا إلى الانحراف ذلك الجهاز عن هدفه الرسمي لصالح أهداف خاصة سواء كان ذلك بصفة متجددة أو مستمرة وساء كان بأسلوب فردي أم بأسلوب جماعي منظم.[14]

- كما عرفه أيضا علماء الاجتماع الفساد بأنها ظاهرة اجتماعية تستخدم بصورة عامة للدلالة على الأعمال التي تخالف القانون بهدف تحقيق منافع خاصة على حساب مصلحة عامة.

حيث عرف حجازي الفساد بأنه: السلوك الذي ينحرف على المعايير والقواعد التي تنظم ممارسة وظيفة عامة أو أداء دور جماعي للحصول على نفع شخصي أو جماعي غير مستحق أو التهاون في الالتزام بمعايير الأداء السليم للواجبات أو تسهيل ذلك للآخرين حيث أن هذا التعريف يركز على الدور الاجتماعي في توجيه السلوك الفاسد.[15]

2- الفساد من ناحية الشريعة الإسلامية:

عنيت الشريعة الإسلامية بحماية كل المصالح العامة للأفراد والمحافظة على الضروريات الخمس التي تعتبر هي الأخرى الحصن الواقي من شتى سبل الفساد فكانت لها بهذا أفضلية

---

[13]- عبد الكريم بن سعد إبراهيم الخثران واقع الإجراءات الأمنية المتخذة للحد من جرائم الفساد من وجهة النظر العاملين في أجهزة مكافحة الرشوة في مملكة العربية السعودية رسالة ماجستير - قسم العلوم الشرطية - جامعة نايف العربية للعلوم الأمنية - الرياض، 2003، ص21.

[14]- حاجة عبد العالي، مرجع سابق، ص20.

[15]- حاجة عبد العالي، مرجع سابق، ص21.

السبق على غيرها من النظم في الوقائي من الفساد لم تتسم به من الشمولية في نصوصها التشريعية في المصالح المحمية ابتداء من العقائد الإيمانية والعبادات وانتهاء بنظمها الاجتماعية والاقتصادية والسياسية.[16]

حيث نظرت الشريعة الإسلامية للفساد بمنظور أشمل وأوسع وذلك من خلال ذكر الفساد في القرآن الكريم في آيات قرآنية وكذا في السنة النبوية من خلال أحاديث نبوية هذا ما سنوضحه في ما يلي:

لقد ورد مصطلح الفساد في العديد من الآيات القرآنية في أكثر من خمسين موضعا بدلالات متعددة وسياقات مختلفة مما يؤكد ان الفساد في القرآن الكريم بتنظيم كل المعاصي والمنكرات التي تخالف ما هو مطلوب شرعا.[17]

فكلمة الفساد نظرا لخطورتها تكررت كثيرا في كتاب الله عز وجل ولكن بأوجه متعددة كلها تبين محاربة الله عزوجل لكافة الفساد وجميع السلوكيات المرتبطة بها من سرقة وقتل ورشوة...إلخ. وتعدي على ممتلكات...الخ. فكما جاء في قول الإمام الغزالي رحمه الله عليه إنما فسدت الرعية بفساد الملوك، وفساد الملوك بفساد العلماء فلولا القضاء السوء والعلماء السوء لقل فساد الملوك خوف من إنكارهم.

لقد جاء ذكر الفساد في الكثير من الأحاديث النبوية الشريفة تناولت موضوع الفساد بصيغة عامة والمفسدين وفيما يلي ذكر لبعض منها:

عن أبو هريرة رضي الله عنه ان رسول الله صلى الله عليه وسلم قال: المتمسك بسنتي عند فساد أمتي له أجر شهيد.[18]

---

[16]– الحاج علي بدر الدين كتاب جرائم الفساد وآليات مكافحتها في التشريع الجزائري – الجزء الأول–دار الأيام–أمة تقرأ... أمة تتقدم ص34.

[17]– بتة بدرة، مكافحة الفساد في الجماعات المحلية في الجزائر، مذكرة نيل شهادة ماستر 2020–2021. ص10.

[18]– الحاج علي بدر الدين مرجع سابق، ص36.

ثالثا: تعريف الفساد من ناحية المنظمات والهيئات الدولية:

تناولت العديد من المنظمات الدولية والهيئات الدولية مصطلح الفساد فكل منها أعطى تعريفات مختلفة عن الفساد وجرائمه إلا أن كلها منكرة لهذا السلوك الهادم للمنظومة العمومية والخاصة للدول وتتمثل هذه التعريفات في ما يلي:

1-تعريف البنك الدولي للفساد:

عمل البنك الدولي على وضع العديد من التعريفات المتعلقة بالفساد من بينها التعريف الآتي: "الفساد هو إساءة استعمال الوظيفة العامة لتحقيق مكاسب خاصة، فالفساد يحدث عادة في ما يلي:

1- عندما يقوم موظف بقبول أو طلب أو ابتزاز رشوة لتسهل عقد أو إجراءات مناقصة عامة.

2- كم يتم عندما يعرض وكلاء أو وسطاء الشركات أو إكمال خاصة بتقديم رشوة للاستفادة من سياسات أو إجراءات عامة للتغلب على منافسين وتحقيق الأرباح.

3- كما يمكن للفساد أن يحدث أو يحصل عن طريق استغلال الوظيفة العامة دون اللجوء إلى على الرشوة بتعيين الأقارب أو سرقة الأموال الدولة مباشرة.[19]

2- تعريف منظمة الشفافية الدولية : الفساد هو كل عمل يتضمن سوء استخدام المنصب العام لتحقيق منفعة ذاتية لنفسه أو لجماعته".[20]

حيث أن منظمة الشفافية الدولية في تعريفها الفساد فرقت بين نوعين ويتمثلا في ما يلي:

[19]- حاجة عبد العالي – مرجع سابق – ص 21-22.

[20]- قارة ملاك – الملتقى الوطني الأول حول الفساد وتأثيره على التنمية الاقتصادية يومي 24-25 افريل 2019- آليات مكافحة الفساد في الجزائر بين النظرية والتطبيق جامعة قسنطينة -02- عبد الحميد مهري ص-3.

– **الفساد بالقانون** حيث يعرف هذا النوع من الفساد حسب المنظمة ب: بمدفوعات التسهيلات التي تدفع فيها الرشاوي وذلك من أجل الحصول على الأفضلية في خدمة يقدمها مستلم الرشوة وفقا القانون.

الفساد ضد القانون : وهو ما يعرف بتقديم رشوة للحصول عن سلم الرشوة على خدمة ممنوع تقديمها.[21]

فالملاحظة أن المنظمة اعتبرت الفساد ذلك السلوك التي ينتج عنه سوء استخدام السلطة العامة لربح منفعة خاصة سواء بالقانون أو ضده.

3- تعريف منظمة الأمم المتحدة للفساد:

جاء تعريف الفساد وفقا لمشروع اتفاقية الأمم المتحدة لمكافحة الفساد2003 بأنه "القيام بأعمال تمثل أداء غير سليم للواجب أو إساءة استغلال لموقع أو سلطة بما في ذلك أفعال أو انفعال توقعا لمزية أو سعيا للحصول على مزية يوعد بها أو تعرض أو تطلب بشكل مباشر أو غير مباشر وأثر قبول مزية ممنوحة بشكل مباشر أو غير مباشر–سواء لشخص ذاته أو لصالح شخص آخر.

كما ان اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية لسنة 2000 أكدت على وجود الفساد غير أن معناه جاء مرادفا للرشوة تمام، وذلك من خلال الماد 08 منها.[22]

4- تعريف منظمة الوحدة الإفريقية للفساد:

اعتبرت منظمة الوحدة الأفريقية ضمن المنظمات الدولية التي سابقت بل اكتفت بالإشارة فقط إلى صوره ومظاهره وذلك من خلال ما جاء في نص المادة منها: على أن يقصد به الفساد:"

---

[21]– بن علي يمينة دور المنظمات الدولية غير الحكومية في مكافحة الفساد (دراسة حالة الشفافية الدولية) – مذكرة ماستر – جامعة خيضر بسكرة 2018–2019– قسم العلوم السياسية وعلاقات دولية.

[22]– حاجة عبد العالي، مرجع سابق، ص22.

الأعمال أو الممارسات بما فيها الجرائم ذات الصلة التي تجرمها الاتفاقية والمشار إليها في المادة 104.[23]

رابعا: تعريف المشرع الجزائري للفساد :

يعتبر مصطلح الفساد مصطلح جديد في التشريع الجزائري ودلالته لا يستعمل قبل سنة 2006 إلى أن شاركت الجزائر في اتفاقية الأمم المتحدة المكافحة الفساد وصادقت عليها في سنة 2004 بموجب المرسوم الرئاسي رقم 128/04 المؤرخ في 19 أفريل2004 هذا ما دفع بالجزائر على وجوب تكييف تشريعاتها بما يتلاءم مع اتفاقية المنظمة لها، من خلال إصدار قانون الوقاية من الفساد ومكافحته 01/06 المؤرخ في 20 فيفري 2006 المعدل والمتمم[24] لكن بالرجوع على هذا القانون نجد انه لم يتضمن تعريف مصطلح الفساد تعريفا فلسفيا أو وصفيا، إنما اكتفى المشرع الجزائري بالإشارة على صور الفساد ومظاهره حيث يظهر هذا من خلال الفقرة أن المادة 02 من القانون 01/06 التي جاء فيها إن الفساد هو :" كل الجرائم المنصوص عليه في الباب الرابع من هذا القانون".[25]

فبالعودة إلى المادة الرابعة من نفس القانون نجد إن المشرع نص على تجريم مجموعة من الافعال بحيث صنفها ضمن جرائم الفساد لعل من بين رشوة الموظفين العموميين إضافة إلى جريمة اختلاس الممتلكات من قبل الموظف العام واستغلال النفوذ...الخ.[26]

الفرع الثاني: أنواع الفساد

1) أنواع الفساد : لقد أصبح الفساد أنواعا كثيرة، تأخذ أشكالا مختلفة تتقاطع فيما بين كثير في النقاط والهوية والتفرقة ارتأيت التقسيم الموضح كالتالي:

---

[23]– بن علي يمينة دور المنظمات الدولية غير الحكومية في مكافحة الفساد عبد العالي، مرجع سابق، ص25.

[24]– حاجة مرجع سابق ص 24.

[25]– المادة 2 من قانون الوقاية من الفساد ومكافحته 06–01 المؤرخ في 20 فيفري 2006 للمعدل والمتمم–الفقر أ.

[26]– خربط محمد –محاضرات قياس مكافحة الفساد – جامعة بليدة كلية الحقوق والعلوم السياسية قسم القانون الخاص– 2020–2021 ص2.

1- الفساد من حيث الحجم

1-1- الفساد الصغير : ويقصد به الفساد الذي يمارس من فرد واحد دون تنسيق مع الآخرين بمعنى إن الفساد يكون أقل حجما وينشر في الهياكل العمومية ذات المستويات المنخفضة ويرتكبه صغار الموظفين من اجل مبالغ مالية بسيطة إلى حد ما.[27]

1-2- الفساد الكبير: هو الفساد الذي يقوم به كبار المسؤولين والموظفين لتحقيق مصالح مادية أو اجتماعية كبيرة وهذا أشمل وأخطر من حيث تكليفه للدولة لمبالغ ضخمة[28]. حيث يصنف هذا النوع من أخطر أنواع الفساد من حيث مقدار الضرر والخسائر التي تنتج عنها.

2- الفساد من حيث الانتشار :

2-1-الفساد المحلي: هو الفساد الذي يكون انتشاره داخل إقليم دولة ما أي في بلد واحد، ويتمثل أطرافه في موظفين عمومين أو أشخاص طبيعية ومعنوية.

2-2-الفساد الدولي: يقصد به الفساد الذي يأخذ أبعادا واسعة تتجاوز الحدود الإقليمية للدولة وتصل إلى نطاق عالمي، حيث يساهم فيه كل من أعوان وموظفون عمومين أجانب- وممثلي المنظمات الدولية داخل الإقليم المحلي كالشركات المتعددة الجنسيات وكذا ممثلي التجارة الدولية صندوق النقد الدولي.[29]

3-الفساد من حيث نوع القطاع:

3-1- فساد القطاع العام هو الفساد التي يظهر انتشاره في الإدارة الحكومية وكذا جميع الهيئات العمومية، حيث أن بشكل أكبر عائق للتنمية نتيجة ما يعرفه من استغلال للمنصب العام بهدف تحقيق أغراض ومصالح شخصية مدمرة للمصالح العامة للدولة.[30]

---

[27]- محاضرات الفساد وأخلاقيات المهنة، ص 11 موقع الالكتروني: Fac.unc.edu-dz

[28]- فوكراش زوبيدة - محاضرات مقياس أخلاقيات للمهنة والفساد جامعة شلف، قسم إدارة أعمال الرياضة-2019-2020 ص15.

[29]- محاضرات الفساد وأخلاقيات المهنة، مرجع سابق، ص 11.

[30]- حاجة عبد العالي، مرجع سابق، ص27.

3-2- الفساد في القطاع الخاص وهو تأثر القطاع الخاص على مجريات السياسة العامة من أجل تحقيق مصالح خاصة، وشخصية كالإعفاء من الضريبة والحصول على إعانة...كل هذا عن طريق استعمال مختلف الوسائل كالرشوة والهدايا .

4-الفساد من حيث المظهر : يقسم الفساد تبعا للمظهر إلى عدة أنواع من الفساد تتخذ أشكالا وأنواعا مختلفة في مجالات الحياة حيث تتمثل هذه الأنواع فيما يلي:

4-1- الفساد الأخلاقي: يقصد به ذلك النوع من الفساد الذي يرتبط بسلوك الإنسان وتصرفاته التي إذا انزلقت وأصبحت سلوكيات سيئة تؤدي به إلى الانحطاط وتجعله يستسلم لكل نزواته ورغباته حتى وإن أدت به إلى الطريق المنحرف وأنزلت من مستواه إلى أقل الدرجات والمراتب باعتبار مخالفة للنظام والآداب التي ميزه الله بها عن باقي مخلوقاته.

4-2- الفساد الاجتماعي: هو ذلك الفساد الذي يصيب المؤسسات الاجتماعية التي أوكل لها المجتمع تربية الفرد وتنشئته كالأسرة والمدرسة والجامعات ... الخ، فإذا كان تنشئته فاسدة تنتهي بفساد اجتماعي تنتج عنه آثار سلبية على الفرد والمجتمع ككل من عدم احترام وكذا الإخلال بالأمن العام.[31]

4-3- الفساد القضائي: هو الانحراف الذي يصيب الهيئات القضائية مما يؤدي إلى ضياع الحقوق وتفشي الظلم واللاعدالة حيث أن هذا النوع من الفساد له صور وتتمثل فيما يلي المحسوبية الوساطة وقبول الهدايا -الرشاوي-شهادة الزور.

فباعتبار أن القضاء هو السلطة التي يهول عليها الناس لإعادة حقوقهم المنتهكة في حين حمايته من الفساد القضائي يؤدي ذلك إلى هلاك الحكومات والشعوب ومبدأ العدالة والنزاهة قضائية.[32]

---

[31]- فوكراش زبيدة، مرجع سابق، ص20.

[32]- حاجة عبد العالي، مرجع سابق، ص 29.

4-3- الفساد السياسي: يعرف الفساد السياسي بأنه تقليب مصلحة صاحب القرار السياسي على مصالح الآخرين والمقصود هنا هو تقديم المصالح الخاصة لصانعي القرار السياسي على المصالح العامة للبلاد ومن أمثلته: فساد الأحزاب السياسية في شراء الأصوات والرشاوي[33] وغيرها من الممارسات التي تعرقل مسار السياسي الديمقراطي للدولة. فبالنظر إلى هذا النوع من الفساد نرى بأنه مظاهره تتعدد وتختلف من دولة إلى أخرى لكن في كل الأحوال فهو يعني فساد طبقة السياسة والحكام وقذارة الأحزاب، حين يقوم هؤلاء باستغلال مواقع النفوذ السياسي بغية زيادة ثروتهم على حساب الشعب ومن خلال نهب المال العام[34]، فالعناد السياسي له العديد من النتائج المدمرة على كافة المستويات لعل من أبرزها: تراجع دور الشعب ومشاركته في الشؤون العامة نتيجة قلة مفهوم المواطنة وأداء الواجب الوطني، الزيادة الملحوظة في الفئات الفقيرة والمهمشة تراجع مستوى الخدمات العمومية نتيجة نهب المال وتهريبه إلى الخارج لاستثمارات خارجية سرية بأموال الشعب.

الفساد الإداري: يتمثل في كل الانحرافات الإدارية وكذا التنظيمية فهو عبارة عن مجموع مخالفات تنتج عن الموظف خلال أداءه لمهامه أو لوظيفة عمومية، ففساد الموظف العام يظهر في العديد من السلوكيات لعل من أبرزها قبول مالا أو هدية ذات قيمة مالية (رشوة)، في مقابل أداء عمل هو ملزم بأدائه وواجب عليه[35]. أو مارس وظيفته بطريقة غير شرعية وقد يكون انحرافه دون قصد بسبب إهمال أو اللامبالاة ويتسبب في فساد إداري، فقد تساهم العديد من الأسباب التي تهدف إلى انتشار هذا النوع قد تكون اقتصادية كنقص الراتب الوظيفي وبالتالي عدم القدرة على الوفاء بمتطلبات المعيشية لأسباب سياسية مرتبطة بعد

---

[33]- محمد جمعة عبدو (الفساد أسبابه....ظواهره .... آثاره والواقية) ملحق الكتاب دراسة عن الحالة الليبية ومؤشراتها من 2010م - 2018م دار المتاب الوطنية ص14.

[34]- عزمي الشعبي، تقرير في إطار مشروع إقليمي في المطبعة العربية - مفوض أمن مكافحة الفساد والآخرون (الفساد السياسي في العالم العربي) - حالة دراسة - حزيران 2014 ص5.

[35]- يوسف عبد عطية، بحر الفساد- الإداري المسببات والعلاج دراسة تطبيقية عن المستشفيات الكبرى في قطاع غزة كلية الاقتصاد - قسم إدارة أعمال جامعة غزة سنة 2011- ص 10.مقالة علمية.

استقرار السياسي والذي يخلف أثره على إدارة العامة نتيجة ممارسته وقد يكون كذلك راجع لأسباب اجتماعية باعتبار أن هناك الكثير من الموظفين نشأوا في بيئة اجتماعية لا تهتم كثيرا بغرس القيم والأخلاق الدينية، وقد يكون أسبابه حتى قانونية في حالة القوانين واللوائح المنظمة للعمل[36]

الفساد المالي: يعتبر الفساد المالي كل أسلوب أو وسيلة غير شرعية يكون الهدف منها سواء الربح السريع أو الحصول على أموال عامة أو خاصة كل هذه التصرفات تحت طائلة الانحراف والانتهاك أو التحايل على الشرع والقانون.

ويمكن تعريفه أيضا بأنه مجموع الانحرافات المالية التي تمس العمل الإداري والمالي للدولة ومؤسساتها والتي تنتج عنها مساس بالمال العام.[37]

فالفساد المالي تتسم أعماله وتصرفاته بالسرية التامة ويمارس بأساليب متعددة ومتطورة بسرعة على حسب التطور التكنولوجي كما يتميز بتقديم المصلحة الخاصة على المصلحة العامة من خلال انتهاك الأموال العامة وخرق القوانين والمسؤوليات المناطة.

– ولفساد المالي كغيره من أنواع الفساد الأخرى له مظاهر تتحد البعض منها فيما يلي:

– الرشوة: التي تعد أكثر ظاهرة يتميز بها الفساد المالي باعتبارها تتوافر على عنصر المال المنفعة فهي تختلف بشكلها وطبيعتها وذلك من خلال قيمة إذا كانت عينية أو مادية.

–الاختلاس: هو السلوك التي يستخدمه الموظف في الاستيلاء على أموال عامة وخاصة خلال أداءه وظيفته.

الفساد الثقافي: يقصد به انحراف جماعة على الثوابت العامة لدى الأمة مما يساهم في تفكيك هويتها وإرثها الثقافي حيث يعتبر الفساد الثقافي فساد بصعب الإجماع على إدانته أو

---

[36]– يوسف عبد عطية، المرجع نفسه، ص10.

[37]– بامحمد عبد القادر وغزوز ياسين متطلبات تفعيل أليات مكافحة الفساد في الجزائر – جامعة أحمد دراية– ادرار الجزائر – قسم العلوم التجارية – مذكرة لنيل شهادة الماستر ميدان علوم اقتصادية وتجارية 2019 – 2020ص6.

سن قوانين او تشريعات تجرمه، عكس أنواع الفساد الأخرى وهذا راجع إلى تحصنه وراء حرية الرأي والتعبير والإبداع[38] رغم كل الانزلاقات التي يحدثها في ثقافة وتقاليد كل دولة على حدى عبر تخريب عقول الناس والترويج للأفكار المستوردة تهدم مقومات الأمة.

الفساد الاقتصادي : هو ذلك الانحراف التي تنتج عنه أعمال تقلب الموازين الاقتصادية وتربك التعامل التجاري، حيث تشمل سلوكياته في أكل أموال الناس بالباطل عبر طرق غير مشروعة وخارجة عن أطر القانونية للتعامل الاقتصادي النزيه منها الغش وتنقيص المكيال والميزان.[39]

فالفساد الاقتصادي ولأنه يؤدي على انتشار الجريمة والفساد وضعت له نصوص قانونية محاربة له في كل تشريعات دول العالم باعتبار أحد أنواع الفساد الخطيرة والصعب علاجها إلا بالأطر القانونية.

المطلب الثاني: مظاهر الفساد المرتبطة بتكنولوجيا المعلومات

لقد ساهم التوسع في استخدام تكنولوجيا المعلومات في تحسين الكفاءة والشفافية داخل المؤسسات، إلا أنه أوجد في المقابل بيئة خصبة لأنواع جديدة من الفساد الرقمي، أضحت تتطلب وعيًا تقنيًا وتنظيميًا عاليًا لرصدها ومعالجتها. وفيما يلي عرض لأبرز مظاهر الفساد المرتبطة بهذا السياق، موزعة على ثلاثة محاور أساسية:

الفرع الأول: التلاعب بالبيانات الرقمية والمعطيات الرسمية

يُعد التلاعب بالبيانات من أخطر مظاهر الفساد المعلوماتي في العصر الحديث إذ يتم عبره وعبر وسائلها وتطبيقاتها المنتشرة بكثرة الى تغيير أو تعديل المعلومات في قواعد البيانات الرسمية بطرق غير قانونية، سواء في صورة تتمثل في هدف إخفاء مخالفات، أو تسهيل حصول أطراف معينة على امتيازات دون وجه حق، ويشمل هذا النوع من الفساد

[38]– حاجة عبد العالي، مرجع سابق، ص 28.

[39]– محمد عباس نعمان الجبروني مفهوم الفساد في القرآن الكريم –جامعة بابل كلية الدراسات القانونية–ص39–مجلة كلية التربية الأساسية أيار 2014.

تعديل سجلات الموظفين أو الجداول المالية داخل الأنظمة. وحذف أدلة رقمية تتعلق بصفقات مشبوهة. والعمل على تزوير الوثائق الرسمية الإلكترونية (كشهادات الميلاد أو كشوف الرواتب)[40].

وقد أظهرت دراسات مثل دراسة **Pfeffer & Sutton (2006)** أن المنظمات التي تفتقر إلى نظام تدقيق رقمي فعال تكون أكثر عرضة لهذا النوع من التلاعب، لأن المعطيات تصبح مرنة بيد الفاعلين داخليًا، دون قدرة على كشف التغيير الزمني أو المتسبب به.

الفرع الثاني: إساءة استخدام الصلاحيات المعلوماتية من قبل الموظفين

تُشكل إساءة استغلال الصلاحيات واحدة من مظاهر الفساد "الداخلية" في المؤسسات والحكومات حيث يقوم بعض الموظفين باستعمال حساباتهم التي هي في الأصل مقدمة لهم من المؤسسة من أجل تقديم الخدمة أو صلاحياتهم للوصول إلى معلومات لا تتصل بمهامهم، أو تمرير بيانات إلى جهات أخرى مقابل منافع شخصية، وقد تتجلى صور هذا السلوك في الولوج غير المصرح به إلى قواعد البيانات الحساسة التي غالبا ما يكون الدخول اليها غير مسموح الا للموظف المسؤول عنها، وقد تظهر في صورة منح صلاحيات الدخول إلى أطراف غير مختصة وليس لها علاقة بالتخصص وقد تكون أيضا في صورة استخدام أنظمة المراقبة الرقمية لمتابعة أو ابتزاز الآخرين.

الفرع الثالث: الفساد في إسناد صفقات التكنولوجيا والرقمنة

غالبًا ما تكون مشاريع الرقمنة والمعلوماتية محل تنافس بين شركات القطاع الخاص ما يجعلها بيئة قابلة للتلاعب إذا غابت الشفافية والحوكمة. ومن بين مظاهر هذا النوع من الفساد اسناد صفقات تصميم أو تطوير أنظمة إلكترونية دون احترام قوانين المنافسة وربما يكون في صورة تضخيم تكاليف البرامج والمعدات المعلوماتية أو إدراج تجهيزات وهمية كما هو الحال الى اعتماد برامج ضعيفة الأداء مقابل عمولات أو رشاوى خفية[41].

---

[40] الشاذلي ياسر، الفساد الإداري في ظل التحول الرقمي .مجلة البحوث الإدارية، جامعة القاهرة، 2018، ص 89.

[41] عبد الله سامي، أمن المعلومات والفساد الرقمي .دار الفكر الجامعي، الإسكندرية، 2020، ص 254.

وتُعد هذه الظاهرة من أبرز التحديات في الدول النامية، حيث أشارت دراسة **Heeks (2006)** حول الفساد في مشاريع الحكومة الإلكترونية، إلى أن نسبة كبيرة من مشاريع الرقمنة تفشل بسبب التلاعب في اختيار المتعاملين، وعدم إخضاع أنظمة الشراء العمومي لمراقبة رقمية فعالة.

خلاصة الفصل :

من خلال هذا الفصل، تم التأسيس للإطار النظري الذي يُعدّ قاعدة أساسية لفهم العلاقة بين الأمن المعلوماتي ومكافحة الفساد، وذلك عبر مقاربة مفهومية وتحليلية شملت توضيح كل من مفاهيم الأمن المعلوماتي والفساد، وإبراز أبعادهما وتشابكهما داخل السياق الرقمي الحديث.

ففي المبحث الأول، تبيّن أن الأمن المعلوماتي ليس مجرد إجراءات تقنية، بل هو منظومة متكاملة تضم مكونات بشرية، تنظيمية، وتقنية، تسعى لحماية المعلومات من التهديدات بكافة أنواعها، وضمان السرية والنزاهة والتوافر. كما تم استعراض أهم الوسائل التقنية الحديثة مثل الجدران النارية، وأنظمة كشف التسلل، وبرمجيات التشفير، وأدوات المصادقة.

أما في المبحث الثاني، فقد تم تحليل مفهوم الفساد ومظاهره التقليدية، وصولًا إلى أشكال جديدة ظهرت في البيئة الرقمية، كالتلاعب بالبيانات، وإساءة استخدام الصلاحيات المعلوماتية، وتسريب المعلومات. وتم عرض المظاهر الخاصة بالفساد المرتبط بتكنولوجيا المعلومات، مثل الفساد في الصفقات الرقمية، وتغليب المصالح الشخصية في منح الامتيازات التقنية. كما تم تسليط الضوء على التهديدات المتزايدة التي تواجه الأمن المعلوماتي في العصر الرقمي، سواء كانت بشرية، تقنية أو تنظيمية.

وقد أكدت محاور هذا الفصل أن مواجهة الفساد في العصر الحديث لم تعد ممكنة دون تأمين البنى المعلوماتية وحماية الأنظمة الرقمية من التلاعب والاختراق، وهو ما يجعل من الأمن المعلوماتي ركيزة أساسية لأي استراتيجية فعالة لمكافحة الفساد.

الفصل الثاني: دور الأمن المعلوماتي في مكافحة الفساد

الفصل الثاني: الأمن المعلوماتي ومكافحة الفساد

تمهيد

في ظل التحديات المتزايدة التي تواجهها الدول والمؤسسات في محاربة الفساد بمختلف صوره وأشكاله، أصبح من الضروري تبنّي وسائل وآليات حديثة تتلاءم مع طبيعة الفساد المعاصر، لا سيما في البيئة الرقمية. فقد أظهرت التجارب الدولية أن الآليات التقليدية لم تعد كافية لردع الممارسات الفاسدة التي باتت تتسلل عبر الأنظمة المعلوماتية والبيانات الرقمية، مستغلة الثغرات التكنولوجية وضعف الحوكمة الإلكترونية.

وفي هذا السياق، برز الأمن المعلوماتي كخيار استراتيجي لا غنى عنه في مواجهة الفساد، من خلال ما يوفره من وسائل تقنية وتنظيمية وإدارية تهدف إلى حماية المعلومات، وتعزيز الشفافية، وضمان سلامة المعاملات الرقمية. كما يساهم في بناء بيئة رقمية آمنة تُقلّل من فرص استغلال الأنظمة والتلاعب بالبيانات، وتُمكّن من تتبع الأنشطة المشبوهة ومحاسبة مرتكبيها.

إن العلاقة بين الأمن المعلوماتي ومكافحة الفساد تتعدى البعد الوقائي إلى البعد الرقابي والردعي، حيث تُسهم أدوات الأمن المعلوماتي في كشف التجاوزات، وتوثيق الأدلة الرقمية، وتحصين المؤسسات ضد التلاعب الداخلي والخارجي. وبالتالي فإن استثمار تكنولوجيا المعلومات في تعزيز منظومات النزاهة والشفافية بات أمرًا حتميًا وليس خيارًا إضافيًا.

وعليه، يهدف هذا الفصل إلى تسليط الضوء على دور الأمن المعلوماتي في مكافحة الفساد من خلال:

المبحث الأول: آليات الأمن المعلوماتي في الوقاية من الفساد

المبحث الثاني: مظاهر تكريس الامن المعلوماتي في مكافحة الفساد

المبحث الأول: آليات الأمن المعلوماتي في الوقاية من الفساد

يُعدّ الأمن المعلوماتي ركيزة أساسية في الوقاية من الفساد داخل البيئة الرقمية، إذ يُمكّن من بناء أنظمة مؤسسية أكثر شفافية وقدرة على رصد المخالفات. وقد ساهم تطور التكنولوجيا في ابتكار أدوات متقدمة تُمكّن المؤسسات من تعزيز منظومات الرقابة، من خلال التتبع، التدقيق، حماية المعطيات، والتحكم في الصلاحيات. ويُبرز هذا المبحث كيف تُسهم النظم التقنية والسياسات الأمنية في خلق بيئة رقمية تُحد من فرص التلاعب والاختراق والفساد الإداري.

المطلب الأول: النظم التقنية كآلية وقائية ضد الفساد

يمثل توظيف النظم التقنية الحديثة في الإدارة الرقمية إحدى أكثر الآليات فعالية في مجال مكافحة الفساد، حيث تمكن هذه النظم من الحد من التلاعب والتزوير، وكشف محاولات الاختراق أو الاستغلال غير المشروع للمعلومة. وفي السياق المؤسساتي، يُعد استخدام أدوات مثل المراقبة الرقمية، والتدقيق الإلكتروني، والتشفير، ومنصات الإبلاغ آليات استراتيجية لتكريس الأمن المعلوماتي وتعزيز الشفافية والمساءلة. في هذا المطلب، نسلط الضوء على أبرز هذه النظم التقنية وآلية عملها في الوقاية من الفساد.

أولا: أنظمة المراقبة الرقمية

تعمل أنظمة المراقبة الرقمية على تتبع جميع الأنشطة التي تتم داخل النظام المعلوماتي للمؤسسات وحتى الحكومات بحيث يتم تسجيل كل عملية دخول، أو تعديل، أو حذف، أو نقل ملفات، أو حتى محاولات الولوج غير المشروع.[42] وبذلك تُوفّر هذه الأنظمة لوحات تحكم تظهر بشكل لحظي المستخدمين النشطين، الإجراءات التي يقومون بها،

[42] موسى، علي، .دور نظم المراقبة الرقمية في الحد من الفساد الإداري .مجلة العلوم الإدارية، جامعة البليدة 2، 2020، ص89.

والمخالفات المحتملة. كما يمكن في ذات السياق برمجتها لإصدار تنبيهات فورية عند رصد نشاط مشبوه، مثل الدخول خارج أوقات العمل، أو محاولة نسخ ملفات حساسة.

يساعد هذا النوع من المراقبة في تحليل السلوكيات الرقمية للموظفين والتعرف على الأنماط غير المعتادة. فعلى سبيل المثال، يمكن كشف محاولة تلاعب عندما يقوم موظف بمراجعة ملفات لا تخص صلاحياته، حيث أن المراقبة المستمرة داخل بيئة رقمية تعتمد على الحوسبة السحابية ساهمت في تقليص التلاعب بنسبة كبيرة بانظمة المعلومات والبيانات، كما هو الحال الى أن تفعيل آلية المراقبة الرقمية في الإدارات المحلية (خاصة عبر أنظمة تسيير الوثائق الإدارية) سمحت بكشف تجاوزات تتعلق بتعديل قرارات إدارية دون ترخيص.

ثانيًا: أنظمة التدقيق الإلكتروني(Audit Trail Systems)

تُعد أنظمة التدقيق الإلكتروني من أدوات الحوكمة التقنية التي تعنى بتوثيق كافة العمليات المنفذة على النظام في المؤسسات العمومية على الخصوص، مع تسجيل معلومات دقيقة حول "من قام؟"، و"متى؟"، و"بأي وسيلة؟." حيث يتكون هذا النظام من سجل زمني تلقائي (Log File) يُخزن فيه كل إجراء، مثل إرسال أو استقبال وثيقة، تعديل ملف، أو حذف معطيات، ويُمكن الرجوع إليه عند الشك في وجود خرق أو مخالفة.

وتكمن أهمية هذه الأنظمة تكمن في أنها تمنع الإنكار فلا يمكن لأي موظف إنكار قيامه بفعل معين، كما أنها توفر دليلًا قانونيًا رقميًا عند حصول خلاف أو شبهة فساد. وتُمكّن الجهات الرقابية من مراقبة الالتزام بالإجراءات التنظيمية. [43]

حيث أن نظام السجل الإلكتروني القابل للتتبع يُعزز من الشفافية والمساءلة، ويُقلل من فرص التملص الإداري.

---

[43] بن صالح زهير، أثر أنظمة التدقيق الإلكتروني في تقليص الفساد الجمركي .مجلة الدراسات القانونية، جامعة وهران، 2021، ص 125.

ثالثًا: التشفير والتوقيع الرقمي

يُعد التشفير وسيلة حيوية لضمان سرية البيانات الرقمية، حيث يقوم بتحويل البيانات الحساسة إلى رموز غير مفهومة إلا من قبل الجهة المخوّلة. ويستخدم هذا الأسلوب على نطاق واسع في المعاملات البنكية، التراسل الحكومي، والصفقات العمومية. فوظيفة التشفير في الوقاية من الفساد تتجلى في منع المتطفلين من الاطلاع على معلومات حساسة (مثل قوائم المستفيدين، أو العقود). وحماية البيانات عند النقل عبر الشبكات العامة، ومنع تغيير محتوى الوثائق دون إذن.

أما في مجال التوقيع الرقمي فهو بمثابة "ختم إلكتروني" يثبت هوية مرسل الوثيقة، ويوفر دليلًا على أن المستند لم يتغير منذ توقيعه. هذه الآلية مهمة خصوصًا في حماية العقود الإلكترونية، وتفويضات الصرف، والقرارات الرسمية. حيث أن الدول التي اعتمدت التشفير والتوقيع الرقمي في بيئتها الإدارية استطاعت تقليص عمليات التزوير بنسب كبيرة فاقت التوقعات، لكن التوقيع الرقمي بالجزائر أن ضعف البنية القانونية والتقنية حال دون الاستفادة الكاملة من هذه الأداة، رغم جاهزيتها التقنية في بعض القطاعات[44].

رابعًا: منصات الإبلاغ الرقمي عن الفساد

تُعتبر منصات التبليغ الرقمي من أبرز أدوات الوقاية المعتمدة في إطار الشفافية الحكومية، حيث تتيح للمواطنين والموظفين تقديم بلاغات حول وقائع الفساد بشكل سري وآمن.

تعتمد هذه المنصات على التشفير الكامل للمراسلات وحماية هوية المبلّغ وأحيانًا الربط بجهات رقابية مستقلة تضمن المتابعة والتحقيق.

[44] حمدي نادية، التوقيع الرقمي كأداة لحماية المعاملات الإدارية في الجزائر .المجلة الجزائرية للحوكمة الإلكترونية، 2019، ص 88.

يُتيح هذا النظام آلية تواصل مباشرة مع الجهات المعنية دون وسطاء، ما يُضعف شبكات الحماية داخل المؤسسات الفاسدة، ويشجع على التبليغ دون خوف فقد كان إدراج هذه المنصات ساهم في رفع نسبة الإبلاغ بنسبة 35% خلال عامين في بعض الدول الإفريقية.

أما في الجزائر، أطلقت هيئة مكافحة الفساد منصة "صرّح" الإلكترونية، كشفت أن ضعف الثقة في فعالية التبليغ، إضافة إلى نقص الحماية التشريعية للمبلغين، حال دون فاعلية استخدامها على نطاق واسع[45].

المطلب الثاني: السياسات الأمنية والحوكمة المعلوماتية كوسيلة ردعية

لا تقتصر مكافحة الفساد في البيئة الرقمية على استعمال التقنيات والأدوات الأمنية فقط، بل تتطلب أيضًا وجود إطار مؤسسي وتنظيمي يُؤطر هذه الأدوات ويُحسن توظيفها بشكل فعال. وتُعتبر السياسات الأمنية والحوكمة المعلوماتية من الركائز الأساسية لضمان فعالية منظومة الأمن المعلوماتي في ردع الممارسات الفاسدة. فبدون سياسة واضحة لإدارة المعلومات وحمايتها، تظل الأنظمة عرضة للاختراق والاستغلال.

تسهم هذه السياسات في بناء قواعد صارمة للتحكم في الوصول، وتحديد المسؤوليات، وتفعيل آليات الرقابة الداخلية، وهو ما يُمكّن من تقليص المساحات الرمادية، وتعزيز الشفافية، وتحقيق المساءلة القانونية لكل المتدخلين في النظام الرقمي[46].

أولًا: السياسات الأمنية الرقمية كأداة تنظيمية للردع

تشمل السياسات الأمنية مجموعة من القواعد والإجراءات التي تُحدد كيفية إدارة أمن المعلومات داخل المؤسسة، وتشمل تصنيف البيانات (سرية، داخلية، عامة). والعمل على ضبط صلاحيات الوصول إلى الملفات والأنظمة. وتحديد الإجراءات الواجب اتباعها في

[45] بن دحمان حفيظة، الإبلاغ الرقمي عن الفساد في الجزائر: بين النظرية والممارسة .مجلة الشفافية والمساءلة، جامعة سطيف 2022، ص 66.

[46] زروقي غنية، أثر السياسات الأمنية على مكافحة الفساد في المؤسسات الجزائرية .مجلة الدراسات القانونية والسياسية، جامعة الجزائر1 ، 2020، ص 89.

حال خرق السياسات. وتكمن قيمة هذه السياسات في أنها: تمنع الاستغلال العشوائي للأنظمة من قبل الموظفين الذين لهم صلاحيات ولوج هذه التطبيقات التي يسمح لهم بدخولها وفقا للمهام والصلاحيات، كما هو الحال الى خلق بيئة قائمة على الرقابة الذاتية والتقيد الإجباري، فهي كأساس لها تستخدم كأساس قانوني في محاسبة المتورطين في أي خرق.

تمثل السياسات الأمنية الرقمية إطارًا ناظمًا يوجه استخدام الموارد المعلوماتية داخل المؤسسة، من خلال وضع قواعد وإجراءات دقيقة تُحدّد كيفية التعامل مع البيانات، وشروط النفاذ إلى الأنظمة، وآليات حماية المعلومات من الاستغلال غير المشروع. فهذه السياسات ليست مجرد وثائق إدارية بل هي مرجعية ملزمة تُمكّن المؤسسة من بناء ثقافة تنظيمية قائمة على الانضباط السيبراني. كما تساعد على ضبط التفاعلات التقنية بين الأفراد والنظم، وتُسهم في تقليص فرص الخطأ البشري أو الإهمال أو الاستغلال العمدي للثغرات. وتكمن فعالية هذه السياسات في كونها أداة ردعية استباقية تضع الحدود الفاصلة بين ما هو مسموح وما هو محظور في الفضاء الرقمي، بما يُمكّن الجهات المعنية من تطبيق قواعد المحاسبة والمساءلة على أساس معايير محددة سلفًا، دون اجتهاد شخصي. ومن هذا المنطلق، تساهم السياسات الأمنية في خلق بيئة مؤسسية محكمة تُقلّ فيها المساحات الرمادية، ويصعب فيها تبرير السلوكيات غير المشروعة أو تمريرها دون أثر رقمي قابل للتتبع.

حيث أن غياب سياسات أمنية مكتوبة في الإدارات على العموم والجزائرية على الخصوص يجعل من السهل على الموظفين استغلال الثغرات أو تحميل المسؤولية لغيرهم من الموظفين في حال حصول تجاوز منهم ، ولهذا إلزام كل المؤسسات بوثيقة سياسة أمن معلومات معتمدة ومعلنة. كما أن وجود سياسة أمنية موثقة هو أول عنصر يُراجع في عمليات التدقيق والاعتماد السيبراني للمؤسسات[47] .

[47] زروقي غنية، المرجع السابق، ص 102.

ثانيًا: الحوكمة المعلوماتية وضبط المسؤوليات الرقمية

تشير الحوكمة المعلوماتية إلى جملة من الآليات والإجراءات التنظيمية التي تُعنى بتأطير كل ما يتعلق بدورة حياة المعلومات داخل المؤسسة، بدءًا من إنتاجها، مرورًا بعملية تخزينها ومعالجتها، وصولًا إلى توزيعها وحمايتها وفقًا لمبادئ منضبطة تستند إلى الشفافية والمساءلة. وتكتسب الحوكمة المعلوماتية أهميتها في البيئة الرقمية من قدرتها على إرساء ضوابط صارمة تحكم التدفق المعلوماتي وتحدد بدقة من له الحق في الوصول إلى المعلومة، وتحت أي شروط، وفي أي إطار زمني.

ويُبنى هذا المفهوم على مجموعة من المبادئ المركزية، لعل أبرزها الفصل الدقيق بين المهام والمسؤوليات التقنية، بما يمنع تداخل الصلاحيات الذي يُعد أحد أبرز مدخلات الفساد المعلوماتي، بالإضافة إلى التحكم في إدارة الحقوق الرقمية لضمان ألا تتجاوز أي جهة نطاقها الوظيفي، إلى جانب فرض إلزامية التوثيق الدوري للعمليات داخل النظام الرقمي، بما يُمكّن من تتبع كافة المعاملات والممارسات ذات الصلة. كما تُعد عملية تتبع سلاسل اتخاذ القرار الرقمي من المكونات الأساسية لهذه الحوكمة، لما توفره من شفافية عالية في تحديد مصادر القرار وتقييم مدى مطابقتها للمعايير التنظيمية، الأمر الذي يضمن المساءلة الفورية عند أي إخلال بالضوابط أو أي انحراف في السلوك المعلوماتي[48]..

ثالثًا: المعايير الدولية كإطار توجيهي

تشكل المعايير الدولية في مجال أمن المعلومات مرجعيات منهجية موحدة تُساعد المؤسسات على بناء سياسات حماية متكاملة ومتناسقة مع أفضل الممارسات العالمية. وتُعد هذه المعايير، مثل سلسلة ISO/IEC و COBITوغيرها، أدوات توجيهية تساعد على تقييم الوضع الراهن للأنظمة الأمنية، وتحديد نقاط الضعف، ووضع خطط للتحسين المستمر. كما

[48] نوار حفيظ، الحوكمة المعلوماتية كآلية لمكافحة الفساد في البيئة الرقمية .مجلة البحوث الاقتصادية والإدارية، جامعة باتنة، 2021، ص 56.

تمنح هذه المعايير إطارًا تنظيميًا واضحًا لتوزيع المهام، وضبط الإجراءات، وتحقيق الانسجام بين الأداء التقني والإداري، الأمر الذي يُقلص من فرص التلاعب أو سوء الاستخدام. وعبر آلياتها في التدقيق الذاتي والتحقق المستمر

حيث تُوفر هذه المعايير وسيلة صارمة للكشف المبكر عن أوجه القصور أو الانحرافات، وتدفع المؤسسات نحو الامتثال والانضباط، مما يجعل منها أداة ردعية غير مباشرة ضد مظاهر الفساد الرقمي. وتبرز أهمية هذه المعايير بشكل خاص في المؤسسات العامة، حيث يُمكن أن تسهم في تحسين الشفافية التشغيلية وتعزيز مصداقية الإجراءات أمام المواطنين والمراقبين على حد سواء، ضمن بيئة رقمية تُمكّن من تقويم الأداء وتثبيت قواعد النزاهة المؤسسية[49].

المطلب الثالث: الاستراتيجيات المتبعة لضمان تحديث وتطوير تدابير الأمن المعلوماتي المتعلقة بالفساد:

تتطلب الاستراتيجيات لضمان تحديث وتطوير تدابير الأمن المعلوماتي بشكل دوري المواكبة التهديدات الجديدة والمتطورة المتعلقة بالفساد تبني عدة متكاملة.

تتطلب الحماية الفعالة من التهديدات السيبرانية تنفيذ برامج مراجعة وتقييم أمنية منتظمة داخل المؤسسات، هذه البرامج تعد ضرورية لتحديد الثغرات الأمنية وتحليل فعالية التدابير الحالية، تشمل هذه الإجراءات إجراء اختبارات اختراق دورية، التي تمثل واحدة من أهم الأساليب لاكتشاف نقاط الضعف في الأنظمة، تنفذ اختبارات الاختراق عادة بواسطة متخصصين أمنيين لتقليد هجمات حقيقية واختبار قدرة النظام على التصدي لها بالإضافة إلى ذلك، يتضمن تقييم الأمان إجراء تحليل شامل لجميع جوانب الأمان، بما في ذلك تقييم التكوينات الأمنية، ومراجعة سياسات الأمان وفحص مدى تنفيذ التحديثات الأمنية بشكل

[49] قروج، مراد، دور الأطر المرجعية الدولية في تحسين الأداء الرقمي الإداري: حالة ولاية الجزائر .المجلة الجزائرية للحكومة الإلكترونية، العدد 10، ص 128.

دوري، هذا النوع من التحليل يساهم في تحديد أي نقاط ضعف أو ثغرات يمكن أن يستغلها المهاجمون، مما يتيح للمؤسسات اتخاذ إجراءات تصحيحية في الوقت المناسب يساعد تنفيذ هذه البرامج بشكل دوري في الحفاظ على مستوى عالي من الأمان ويضمن أن تدابير الحماية الحالية تظل فعالة ضد التهديدات الجديدة والمتطورة، هذه الإجراءات تضمن أيضاً أن الأنظمة والبيانات تظل محمية من الهجمات السيبرانية التي قد تستهدف نقاط الضعف الموجودة[50]

تعتبر متابعة أحدث التطورات في مجال الأمن المعلوماتي وتحديث أدوات وبرامج الأمان بشكل مستمر من الخطوات الأساسية لضمان حماية فعالة ضد التهديدات السيبرانية المتطورة في ظل التطورات السريعة في هذا المجال، يصبح من الضروري للمؤسسات دمج تقنيات جديدة مثل الذكاء الاصطناعي والتحليل المتقدم في نظم الرصد المواكبة أساليب الهجوم الحديثة ، تقدم تقنيات الذكاء الاصطناعي إمكانيات متقدمة في تحليل البيانات واكتشاف الأنشطة غير الطبيعية، من خلال استخدام خوارزميات التعلم الآلي، يمكن لهذه التقنيات التعرف على الأنماط السلوكية المشبوهة والتنبؤ بالتهديدات قبل حدوثها، هذا يسمح بالاستجابة السريعة والتصدي للهجمات السيبرانية بشكل أكثر فعالية بالإضافة إلى الذكاء الاصطناعي، فإن دمج التحليل المتقدم في نظم الرصد يعزز القدرة على معالجة كميات كبيرة من البيانات بشكل فعال، تقنيات التحليل المتقدم توفر رؤى قيمة حول التهديدات المحتملة، مما يساعد في تحسين استراتيجيات الأمان واتخاذ قرارات مبنية على بيانات دقيقة ، تحديث أدوات وبرامج الأمان بشكل مستمر يعني أيضاً تطبيق أحدث التصحيحات والتحديثات الأمنية التي تطلقها الشركات المصنعة، هذه التحديثات غالباً ما تحتوي على إصلاحات المشاكل أمان مكتشفة حديثاً، مما يعزز الحماية ضد الثغرات التي قد يستغلها المهاجمون بالتالي، تبني هذه التقنيات والممارسات يساهم بشكل كبير في تعزيز قدرة

[50] عبد الحميد منصور، الأمن السيبراني: حماية الأنظمة الرقمية في العصر الحديث" ، ط (1) ، دار الفكر العربي القاهرة، مصر، 2022م ، ص 45

المؤسسات على التصدي لأحدث أساليب الهجوم المعلوماتي وضمان مستوى عال من الأمان[51]

تطوير برامج تدريب مستمرة لموظفي المؤسسات حول أحدث أساليب الحماية والأمن المعلوماتي يعد من العناصر الأساسية للحفاظ على أمان المعلومات وحمايتها من التهديدات المتطورة. يتطلب هذا النوع من التدريب أن يكون دورياً وشاملاً لتلبية التغيرات السريعة في مشهد الأمن المعلوماتي ، يعزز التدريب المنتظم الوعي الأمني بين الموظفين، حيث يساعدهم على فهم طبيعة التهديدات السيبرانية الحديثة مثل هجمات التصعيد الاحتيالي والبرمجيات الخبيثة من خلال تزويد الموظفين بالمعرفة حول كيفية التعرف على هذه التهديدات وكيفية التصرف بشكل مناسب، يمكن للمؤسسات تقليل مخاطر الأمان المرتبطة بالخطأ البشري بالإضافة إلى ذلك، يشمل التدريب تعليم الموظفين حول السياسات والإجراءات الأمنية الخاصة بالمؤسسة، مما يضمن أنهم يتبعون أفضل الممارسات للحفاظ على أمان المعلومات، يمكن أن يتضمن التدريب أيضاً محاكاة لهجمات حقيقية لتقييم مدى استعداد الموظفين وكيفية استجابتهم في حالة حدوث اختراقات من خلال تطوير برامج تدريب مستمرة، تضمن المؤسسات أن موظفيها يظلون على دراية بأحدث أساليب الحماية ويكونون مجهزين للتعامل مع التهديدات السيبرانية بفعالية، هذه البرامج تسهم في بناء ثقافة أمان قوية داخل المؤسسة، مما يقلل من المخاطر المحتملة ويحسن من استجابة المؤسسة تجاه الهجمات السيبرانية

تعتبر إقامة شراكات مع خبراء الأمن المعلوماتي وشركات التكنولوجيا المتقدمة استراتيجية حيوية لتعزيز حماية المؤسسات من التهديدات السيبرانية، توفر هذه الشراكات دعماً متخصصاً في تحليل التهديدات وتطوير استراتيجيات أمان متقدمة مما يساعد المؤسسات على مواكبة أحدث الأساليب والتقنيات في مجال الأمان المعلوماتي ، الخبراء

[51] عبد الله بن صالح الجهني ، الأمن السيبراني وأثره في تعزيز الشفافية ومكافحة الفساد، ط (1) ، دار المريخ للنشر، الرياض، 2023م ، ص 95

في مجال الأمن المعلوماتي يتمتعون بمهارات ومعرفة متعمقة في تحليل التهديدات السيبرانية وتقييم المخاطر، من خلال التعاون معهم، يمكن للمؤسسات الاستفادة من خبراتهم لتحديد الثغرات الأمنية المحتملة وتطوير استراتيجيات حماية مخصصة، هؤلاء الخبراء يقدمون أيضاً تحليلاً مستمراً للتهديدات الناشئة ويوفرون استشارات حول كيفية تعزيز الأمان بشكل فعال تلعب شركات التكنولوجيا المتقدمة أيضاً دوراً أساسياً في تطوير وتنفيذ حلول الأمان الحديثة، من خلال الشراكة مع هذه الشركات، يمكن للمؤسسات الوصول إلى أحدث أدوات وتقنيات الأمان التي تساهم في تعزيز القدرة على التصدي للهجمات السيبرانية، هذه الشركات توفر أيضاً دعما في تكامل هذه الحلول ضمن البنية التحتية التقنية للمؤسسة وضمان توافقها مع احتياجات الأمان المحددة ، تعزز الشراكات مع هذه الجهات المتخصصة من قدرة المؤسسات على تحسين استراتيجيات الأمان الخاصة بها، والتعامل بشكل أكثر فعالية مع التهديدات المتطورة، وتقديم حلول مبتكرة للحفاظ على أمن المعلومات[52]

مما سبق يتضح أنه لتحديث وتطوير تدابير الأمن المعلوماتي بشكل دوري لمواكبة التهديدات الجديدة والمتطورة المتعلقة بالفساد، يجب على المؤسسات تبني مجموعة من الاستراتيجيات الشاملة، تشمل هذه الاستراتيجيات إجراء تقييمات أمنية دورية للكشف عن الثغرات وتحديث الأدوات الأمنية بانتظام لتواكب أحدث التقنيات والتطورات في مجال الأمان المعلوماتي ، من الضروري أيضاً تعزيز برامج التدريب المستمرة لموظفي المؤسسة لرفع مستوى الوعي لديهم حول أحدث أساليب الحماية وأحدث التهديدات بالإضافة إلى ذلك، يجب إقامة شراكات مع خبراء الأمن المعلوماتي وشركات التكنولوجيا المتقدمة للحصول على استشارات متخصصة وتطوير استراتيجيات أمان متطورة، هذه الاستراتيجيات تساهم في

[52] فهد بن سعود العتيبي ، الأمن السيبراني وحماية المعلومات في مكافحة الفساد، ط (2) ، دار المعرفة للنشر، الرياض 2023م ، ص 130

تعزيز قدرة المؤسسات على التعامل بفعالية مع التهديدات السيبرانية وحماية المعلومات الحيوية من المخاطر المتزايدة.[53]

[53] أحمد عبد الرحمن محمد ، تحليل البيانات في مكافحة الفساد وتعزيز الأمان السيبراني، ط (2) ، دار الفكر العربي، القاهرة 2023م ، ص 130

المبحث الثاني: مظاهر تكريس الامن المعلوماتي في مكافحة الفساد

لقد أصبح الأمن المعلوماتي في العصر الرقمي أكثر من مجرد وسيلة تقنية لحماية المعطيات والأنظمة، بل تحوّل إلى أداة حقيقية لتكريس النزاهة وتعزيز ممارسات الشفافية في المؤسسات العمومية والخاصة. فتنامي حجم الفساد، خاصة في البيئة الرقمية، أوجب على الدول والمؤسسات إرساء ثقافة أمن معلوماتي راسخة، لا تقتصر على الجانب التقني، وإنما تمتد إلى بعد إداري وتشريعي ومجتمعي.

وفي هذا السياق، لا يقتصر دور الأمن المعلوماتي على الكشف عن مظاهر الفساد أو الوقاية منه، بل يتجلى كذلك في إرساء آليات بنيوية مستدامة تعزّز مناعة المؤسسات تجاه الاختراقات، وتُكرّس مبادئ الحوكمة الرشيدة

ومن خلال هذا المبحث إلى تسليط الضوء على أهم المظاهر التطبيقية التي يُجسد من خلالها الأمن المعلوماتي دوره في مكافحة الفساد **(المطلب الأول)** تأثير الأمن المعلوماتي على تعزيز الشفافية والحوكمة الرشيدة في المؤسسات

المطلب الأول: تأثير الأمن المعلوماتي على تعزيز الشفافية والحوكمة الرشيدة في المؤسسات

يلعب الأمن المعلوماتي يلعب دورًا مهما في تعزيز الشفافية والحوكمة الرشيدة في المؤسسات عبر مجموعة من الآليات المتكاملة وذلك على النحو الآتي:

يتم تأمين المعلومات والبيانات الحساسة ضد الوصول غير المصرح به والتلاعب مما يساهم في ضمان دقة وسلامة المعلومات التي تعتمد عليها المؤسسات في اتخاذ قراراتها، هذا التأمين يعزز ثقة الأطراف المعنية ويقلل من فرص الفساد، حيث يحافظ على نزاهة البيانات المالية والإدارية، ويمنع التلاعب الذي قد يؤثر سلباً على مصداقية المؤسسة علاوة على ذلك، يوفر الأمن المعلوماتي آليات فعالة للرصد والمراقبة، مما يسهم في تعزيز الشفافية، تقنيات المراقبة والتتبع تتعقب الأنشطة والعمليات داخل النظام وتقدم إشعارات حول أي نشاط غير معتاد أو مشبوه، هذا النوع من الرقابة يمكن المؤسسات من اكتشاف

المشكلات مبكرًا وتحليل مصادر أي خرق أو تلاعب مما يعزز القدرة على اتخاذ الإجراءات التصحيحية الفورية ويشجع على التزام أعلى بالمعايير الأخلاقية ويعزز الأمن المعلوماتي أيضا الحوكمة الرشيدة من خلال ضمان حماية البيانات والامتثال للمعايير القانونية والتنظيمية تعتمد المؤسسات التي على أطر أمان قوية تستطيع تقديم نماذج حوكمة فعالة، مما يدعم الشفافية ويعزز الثقة بين أصحاب المصلحة كما أن الالتزام بمعايير الأمان المعلوماتي يعكس جدية المؤسسة في اتباع سياسات وإجراءات حوكمة دقيقة ومتبعة[54]

تتيح تقنيات الأمن المعلوماتي للمؤسسات تنفيذ آليات مراقبة دقيقة وشفافة من خلال استخدام أنظمة الرصد والتتبع التي تجمع وتحلل الأنشطة والعمليات داخل الشبكات والأنظمة المعلوماتية تساعد هذه الأنظمة على الكشف المبكر عن أي نشاط غير معتاد أو مشبوه، مما يعزز من قدرة المؤسسة على الحفاظ على أمان المعلومات وموثوقيتها بفضل أدوات الرصد والتتبع، تستطيع المؤسسات مراقبة تدفق البيانات والتفاعل بين المستخدمين والأنظمة، مما يوفر رؤية شاملة حول كيفية استخدام الأنظمة ومعالجة البيانات، عند حدوث أي نشاط غير عادي، مثل محاولات الوصول غير المصرح به أو تغييرات غير مبررة في البيانات، تقوم الأنظمة بإصدار تنبيهات تساعد الفرق الأمنية في التحقيق السريع، يعزز هذا المستوى من الرقابة الشفافية داخل المؤسسة لأنه يوفر سجلات دقيقة عن جميع الأنشطة والتفاعلات، مما يسهل تتبع العمليات وتحديد مصدر أي خرق أو تلاعب من خلال تحسين الشفافية عبر هذه التقنيات تصبح المؤسسات أكثر قدرة على اتخاذ القرارات المستنيرة وتصحيح أي مشكلات بسرعة، كما أن هذه القدرة على الرصد والتحليل تساعد في بناء ثقة أكبر بين

[54] محمد حسن الخطيب، الأمن السيبراني وأثره على الشفافية والحوكمة في المؤسسات، ط (1) ، دار النشر العربي، بيروت، 2023م ، ص 120

المؤسسة وأصحاب المصلحة، حيث يتمكن الجميع من رؤية الإجراءات المتبعة في حماية البيانات وضمان عدم وجود أي تلاعب[55]

عندما تضمن المؤسسات سلامة البيانات من خلال تقنيات الأمن المعلوماتي وتمنع الوصول غير المصرح به، فإنها تعزز بشكل كبير من جودة الحوكمة الرشيدة، توفر الأطر الأمنية القوية حماية متكاملة للبيانات والمعلومات الحساسة، مما يقلل من المخاطر التي قد تؤثر على نزاهة المعلومات وسلامتها، بفضل هذه الحماية، يمكن للمؤسسات أن تظهر التزامها بالمعايير الدولية للأمان، مما يعكس التزامها بالشفافية والامتثال للمعايير القانونية والتنظيمية ، تدعم تقنيات الأمن المعلوماتي السياسات والإجراءات الخاصة بالحوكمة من خلال تقديم أدوات وتقنيات تساهم في حماية البيانات وضمان استخدامها بشكل آمن وفعال، من خلال تطبيق أطر أمنية قوية تساهم المؤسسات في بناء نماذج حوكمة فعالة وواضحة، حيث يكون هناك مراقبة مستمرة وتحكم دقيق في الوصول إلى المعلومات، يعزز هذا الأمر من ثقة الأطراف المعنية في قدرة المؤسسة على حماية بياناتها والامتثال للمعايير التنظيمية، مما يعكس مستوى عال من المسؤولية والاحترافية في إدارة المعلومات[56]

مما سبق يؤثر الأمن المعلوماتي بشكل كبير على تعزيز الشفافية والحوكمة الرشيدة في المؤسسات عبر توفير حماية متكاملة للبيانات والمعلومات من خلال ضمان سلامة البيانات ومنع الوصول غير المصرح به، يمكن للمؤسسات أن تضمن أن المعلومات التي تعتمد عليها في عمليات اتخاذ القرارات تكون دقيقة وآمنة، هذا الأمان يعزز من الشفافية لأنه يتيح لجميع الأطراف المعنية متابعة وتحليل الأنشطة والبيانات بوضوحمما يقلل من فرص التلاعب والفساد علاوة على ذلك، تساهم تقنيات الأمن المعلوماتي في تعزيز الحوكمة الرشيدة من خلال تقديم أدوات فعالة للرصد والتحليل، مما يسهم في مراقبة

[55] محمد بن عبد الله الراجحي ، الأمن السيبراني ودوره في تعزيز الشفافية والتعاون الدولي في مكافحة الفساد، ط (1) ، دار الفكر العربي القاهرة 2024م ، ص 104

[56] عبد الله بن صالح الجهني، الأمن السيبراني وأثره في تعزيز الشفافية والحوكمة، ط (1) ، دار الفكر العربي، الرياض، 2023 م ، ص 63

الإجراءات واتخاذ القرارات بشكل مستنير، تستطيع المؤسسات التي تعتمد على أطر أمنية قوية أن تظهر التزامها بالمعايير الدولية، مما يعزز من مستوى الثقة بينها وبين أصحاب المصلحة، هذه الحوكمة الواضحة والفعالة، التي تدعمها سياسات أمان متقدمة، تدعم الامتثال للمعايير القانونية والتنظيمية، وتؤكد على المسؤولية والاحترافية في إدارة المعلومات.

المطلب الثاني: الأمن المعلوماتي وتوفير منصات آمنة للمبلغين عن الفساد وتعزيز التعاون الدولي في مكافحة الفساد:

يلعب الأمن المعلوماتي دورًا حيويًا في توفير منصات آمنة للمبلغين عن الفساد وتعزيز التعاون الدولي في مكافحة الفساد من خلال عدة آليات متكاملة.

يلعب الأمن المعلوماتي دورا حاسما في إنشاء منصات آمنة للمبلغين عن الفساد من خلال توفير بيئة تحمي المعلومات الشخصية للمبلغين وتضمن سرية بلاغاتهم، تقنيات التشفير تشكل الأساس في هذا السياق، حيث تقوم بتحويل البيانات إلى صيغة مشفرة بحيث لا يمكن الوصول إليها أو فهمها إلا من قبل الأشخاص المصرح لهم فقط، هذا يضمن أن تفاصيل البلاغات تظل محمية من الوصول غير المصرح به، مما يقلل بشكل كبير من مخاطر الانتقام أو التعرض للأذى الذي قد يتعرض له المبلغون إذا تم الكشف عن هويتهم أو محتوى بلاغاتهم إضافة إلى ذلك، فإن أنظمة المصادقة المتقدمة تساهم في تعزيز أمان هذه المنصات من خلال التأكد من أن الأشخاص الذين يستخدمونها هم من يمتلكون الصلاحية للوصول إليها، هذه الأنظمة تعتمد على تقنيات متعددة مثل التحقق الثنائي أو البيومتري لضمان أن المبلغين يمكنهم تقديم بلاغاتهم بطريقة آمنة دون خوف من كشف هويتهم، بمعنى آخر، تساهم أنظمة المصادقة في حماية هوية المبلغين من خلال التأكد من أن الوصول إلى المنصات يتم فقط من قبل الأشخاص الذين يمتلكون التصاريح المناسبة بفضل هذه التدابير الأمنية، يتمكن المبلغون من الإبلاغ عن الفساد بارتياح وبدون خوف مما يشجعهم على تقديم بلاغاتهم ويعزز من فعالية مكافحة الفساد الأمن المعلوماتي ، من

خلال هذه الآليات، يعزز الثقة في المنصات المستخدمة للإبلاغ عن الفساد ويعزز من قدرة المؤسسات على معالجة البلاغات بشكل فعال وأمن[57]

يقدم الأمن المعلوماتي أدوات فعالة لرصد وتحليل البلاغات الواردة، مما يعزز من قدرة المؤسسات على فحص هذه البلاغات والتحقق من صحتها بشكل أسرع وأكثر دقة، تستطيع الأنظمة المتقدمة للرصد والتحليل تحليل الأنشطة المشبوهة بفعالية، مما يوفر رؤى دقيقة للمحققين ويساعد في الكشف عن الأنشطة غير القانونية أو الفاسدة، تعمل هذه الأدوات على تسريع عملية معالجة البلاغات، مما يتيح اتخاذ إجراءات فعالة المكافحة الفساد بشكل أكثر كفاءة فيما يتعلق بالتعاون الدولي، يلعب الأمن المعلوماتي دورا حيويا في تسهيل تبادل المعلومات بين الدول والمنظمات من خلال تأمين قنوات الاتصال الدولية، يتيح الأمن المعلوماتي تبادل المعلومات حول الأنشطة الفاسدة والجرائم الاقتصادية بشكل أمن وفعال، كما تساهم تقنيات الأمان المعلوماتي في إنشاء شبكات تعاون عالمية تعتمد على أطر أمان مشتركة، مما يعزز من التنسيق بين الدول والهيئات الدولية، هذه الأطر توفر بيئة محمية لتبادل المعلومات والتحقيق في قضايا الفساد عبر الحدود، مما يدعم جهود مكافحة الفساد بشكل منسق وعالمي بفضل هذه التدابير، يعزز الأمن المعلوماتي من قدرة المؤسسات على معالجة البلاغات بفعالية، ويحسن التعاون الدولي في مكافحة الفساد، ويعزز الشفافية على مختلف الأصعدة[58]

يتضح مما سبق أن الأمن المعلوماتي يلعب دورا أساسيا في تحسين فعالية مكافحة الفساد وتعزيز الشفافية من خلال توفير أدوات متقدمة لرصد وتحليل البلاغات الواردة من خلال تأمين بيانات البلاغات وحمايتها، تتيح تقنيات الأمن المعلوماتي فحصها والتحقق من صحتها بسرعة ودقة، مما يساهم في معالجة الأنشطة المشبوهة بفعالية. هذه الأنظمة توفر رؤى دقيقة تساعد المحققين في اتخاذ قرارات مستنيرة واتخاذ إجراءات سريعة لمكافحة الفساد

57

58

بالإضافة إلى ذلك، يعزز الأمن المعلوماتي التعاون الدولي من خلال تأمين قنوات التواصل بين الدول والمنظمات، هذا التأمين يتيح تبادل المعلومات حول الأنشطة الفاسدة والجرائم الاقتصادية بشكل أمن وفعال ويعزز من التنسيق بين الدول والهيئات الدولية، عبر إنشاء شبكات تعاون عالمية تستند إلى أطر أمان مشتركة، يصبح من الممكن تنسيق جهود مكافحة الفساد بشكل أكثر تنظيماً وفعالية بفضل هذه الجهود، يسهم الأمن المعلوماتي في دعم الجهود العالمية لمكافحة الفساد، مما يعزز الشفافية ويؤدي إلى تحسين إدارة المعلومات عبر مختلف المستويات.[59]

[59] خالد بن إبراهيم الفهد الشراكات الاستراتيجية في الأمن السيبراني تعزيز الأمان من خلال التعاون ، ط (1) ، دار المعرفة التقنية، دبي 2023م ، ص 120

خلاصة الفصل :

تكشف المعالجة النظرية والتحليلية لهذا الفصل عن الأهمية الاستراتيجية التي يكتسيها الأمن المعلوماتي كمنظومة متكاملة في الوقاية من الفساد ومكافحته، ضمن بيئة رقمية متسارعة تُعيد تشكيل أساليب العمل الإداري وميكانيزمات الرقابة. وقد بيّن المبحث الأول كيف أن آليات الأمن المعلوماتي تمثل خط الدفاع الأول في الحد من مظاهر الفساد، وذلك عبر توظيف النظم التقنية الحديثة كوسائل وقائية قادرة على رصد السلوكيات المشبوهة وضبط النشاطات الرقمية داخل المؤسسات، مما يسمح بتقليص هامش المناورة والتحايل الإداري. كما أكد على الدور المركزي للسياسات الأمنية والحوكمة المعلوماتية كأدوات تنظيمية وردعية، تضبط من خلالها المسؤوليات الرقمية وتؤسس لثقافة مؤسساتية قائمة على الانضباط والشفافية. وقد استُكمل ذلك باستعراض الاستراتيجيات المعتمدة لتحديث وتطوير منظومة الأمن المعلوماتي، من خلال إدماج المعايير الدولية، وتعزيز القدرات البشرية، وتبني الحلول السيبرانية المتقدمة، بما يعزز الجاهزية المؤسسية في مواجهة التهديدات المرتبطة بالفساد.

أما المبحث الثاني فقد تناول أبرز مظاهر تكريس الأمن المعلوماتي في مجال مكافحة الفساد، مبرزًا أثره الفعلي في ترسيخ مبادئ الشفافية والحوكمة الرشيدة، باعتبار أن حماية البيانات وتوثيق العمليات رقمياً يسمحان بتقليص التدخلات البشرية غير المشروعة ويُوفران قاعدة موضوعية للمساءلة. كما تم التطرق إلى أهمية الأمن السيبراني في توفير بيئة رقمية آمنة تُمكّن من إطلاق منصات فعالة للتبليغ عن الفساد، بما يضمن حماية المبلّغين ويشجع على كشف المخالفات من داخل المؤسسات نفسها. علاوة على ذلك، أبرز الفصل أهمية تعزيز التعاون الرقمي الدولي وتبادل المعلومات والخبرات بين الدول والهيئات المعنية، في سبيل مواجهة التحديات العابرة للحدود التي يفرضها الفساد في شكله الإلكتروني.

ويمكن القول في المجمل، إن الأمن المعلوماتي لم يعد خيارًا تقنيًا فقط، بل أصبح ضرورة مؤسسية ملحة في ظل التحولات الرقمية، تستوجب تكامل الجوانب التقنية والتنظيمية والتشريعية لضمان نجاعة الجهود الموجهة نحو مكافحة الفساد، وتحقيق مستويات أعلى من النزاهة والشفافية داخل المؤسسات.

الخاتمة

الخاتمة

في خضم التحول الرقمي العميق الذي يشهده العالم اليوم، لم يعد الفساد محصورًا في صيغته التقليدية، بل بات يتخذ أشكالًا أكثر تعقيدًا ومرونة بفعل تكنولوجيا المعلومات والاتصال. وفي هذا السياق، يبرز الأمن المعلوماتي كأحد المرتكزات الجوهرية في منظومة الحوكمة الحديثة، ليس فقط لحماية البيانات والمعلومات، بل كآلية استراتيجية لكشف التجاوزات، وضبط الممارسات الإدارية، وتعزيز الشفافية والمساءلة في مختلف مؤسسات الدولة.

لقد أظهر البحث أن النظم التقنية الحديثة، وعلى رأسها أنظمة المراقبة الرقمية، التشفير، التدقيق الإلكتروني، ومنصات الإبلاغ، تُشكّل أدوات وقائية فعالة تُقلّص من مساحات التلاعب وتُعزّز من القدرة على الردع المؤسساتي. كما أن السياسات الأمنية المكتوبة والحوكمة المعلوماتية تُعدان من أهم آليات التنظيم والرقابة التي تضمن سير العمليات الإدارية في إطار قانوني محكم، يحدّ من فرص التلاعب الرقمي.

ومن جهة أخرى، أثبتت الدراسة أن تعزيز الأمن المعلوماتي يُسهم بشكل ملموس في ترسيخ مبادئ الشفافية، ويُسهل تقييم الأداء، ويوفّر بيئة آمنة للتبليغ عن المخالفات، وهو ما يكرّس مفهوم النزاهة المؤسسية الرقمية ويُعزز ثقة المواطن في الإدارة. كما يُعد الأمن السيبراني، بتقنياته العابرة للحدود، إطارًا حيويًا لتقوية التعاون الدولي في مواجهة الأبعاد العابرة للفساد الإلكتروني، خاصة في ظل اتساع رقعة الفضاء الرقمي وتشابك مصالح الفاعلين الدوليين.

وبناء على ما سبق، يُمكن التأكيد أن تكريس مكافحة الفساد في العصر الرقمي لا يمكن أن يتم بمعزل عن بناء منظومة أمن معلوماتي فعالة، تُزاوج بين التقنيات الحديثة، والإرادة السياسية، والأطر التنظيمية الصارمة. وهذا يفرض على المؤسسات – خاصة في الدول النامية – تبني استراتيجية وطنية شاملة للأمن السيبراني، تُدمج فيها جوانب الوقاية، الحوكمة، والتعاون المحلي والدولي، من أجل تجفيف منابع الفساد الرقمي، وتأمين بيئة رقمية شفافة وآمنة ومستدامة.

النتائج:

1 – أشارت نتائج الدراسة أن الأمن السيبراني يعزز مكافحة الفساد من خلال توفير أدوات متقدمة لرصد وتحليل البلاغات بسرعة ودقة، مما يساعد في معالجة الأنشطة المشبوهة بشكل فعال كما يسهم في تعزيز التعاون الدولي بتأمين تبادل المعلومات بين الدول والمنظمات، مما يتيح تنسيق جهود مكافحة الفساد بشكل آمن وفعال.

2– أظهرت نتائج الدراسة أن الأمن السيبراني يعزز الشفافية والحوكمة الرشيدة في المؤسسات من خلال تأمين البيانات وحمايتها، مما يضمن دقة المعلومات وسلامتها، كما يوفر أدوات لرصد الأنشطة وتحليلها، مما يتيح مراقبة فعالة للعمليات ويساهم في تطبيق معايير حوكمة قوية.

–3 – بينت نتائج الدراسة أن الأمن السيبراني يوفر منصات آمنة للمبلغين عن الفساد من خلال حماية معلوماتهم وتشفير بلاغاتهم، مما يقلل من مخاطر الانتقام، كما يعزز التعاون الدولي بتأمين تبادل المعلومات بين الدول والمنظمات، مما يسهم في تنسيق جهود مكافحة الفساد بشكل فعال.

4– أكدت نتائج الدراسة أنه لضمان الاستراتيجيات تتطلب تحديث وتطوير تدابير الأمن السيبراني بشكل دوري أن تقوم المؤسسات بإجراء تقييمات أمنية دورية، تحديث
أدوات الأمان بانتظام، تعزيز برامج التدريب المستمرة للموظفين، وإقامة شراكات مع خبراء الأمن السيبراني وشركات التكنولوجيا المتقدمة.

التوصيات:

–1–تطبيق تقنيات التشفير لضمان سرية المعلومات والبلاغات المقدمة عن الفساد.

–2استخدام أنظمة المصادقة المتقدمة لضمان وصول المصرح لهم فقط إلى منصات الإبلاغ عن الفساد.

–توفير برامج تدريبية للمستخدمين حول أمان المعلومات وطرق الحماية من التهديدات السيبرانية.

-4تطبيق حلول مراقبة وتحليل متقدمة لرصد الأنشطة المشبوهة والتحقق من البلاغات بسرعة.

-5-إنشاء قنوات اتصال آمنة بين الهيئات والمؤسسات لتبادل المعلومات حول الأنشطة الفاسدة.

-6تحديث برامج الأمان بشكل دوري لمواكبة التطورات في أساليب الهجوم السيبراني.

-7تطوير سياسات أمان قوية تحدد كيفية التعامل مع البيانات الحساسة ومعلومات المبلغين.

-8إجراء مراجعات أمنية منتظمة لتقييم فعالية التدابير الأمنية واكتشاف الثغرات.

- 9تعزيز الشفافية في العمليات الأمنية من خلال تقديم تقارير دورية حول نشاطات الأمن السيبراني.

-10-تشجيع التعاون بين القطاعين العام والخاص لتبادل المعرفة والخبرات في مجال الأمان السيبراني.

-11-توفير أدوات تحليل بيانات متقدمة لتحليل الأنشطة المشبوهة وتحديد الأنماط المرتبطة بالفساد.

-12- تطبيق تقنيات الذكاء الاصطناعي في الرصد والكشف المبكر عن الأنشطة غير العادية.

قائمة المراجع

أولا: الكتب

1. أحمد عبد الرحمن محمد، **تحليل البيانات في مكافحة الفساد وتعزيز الأمان السيبراني**، ط2، دار الفكر العربي، القاهرة، مصر، 2023.
2. الحاج علي بدر الدين، **جرائم الفساد وآليات مكافحتها في التشريع الجزائري**، الجزء الأول، دار الأيام للنشر والتوزيع.
3. خليف فوزي، **أمن المعلومات في البيئة الرقمية**، دار الكتب العلمية، الجزائر، 2022.
4. رابح محمد، **الجرائم المعلوماتية وأمن النظم الإلكترونية**، دار الهدى للنشر والتوزيع، مصر، 2021.
5. عبد الرحمن شعبان عطيات، **أمن الوثائق والمعلومات**، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
6. عبد الحميد منصور، **الأمن السيبراني: حماية الأنظمة الرقمية في العصر الحديث**، ط1، دار الفكر العربي، القاهرة، 2022.
7. عبد الله بن صالح الجهني، **الأمن السيبراني وأثره في تعزيز الشفافية ومكافحة الفساد**، ط1، دار المريخ للنشر، الرياض، 2023.
8. عبد الله بن صالح الجهني، **الأمن السيبراني وأثره في تعزيز الشفافية والحوكمة**، ط1، دار الفكر العربي، الرياض، 2023.
9. عبد الله سامي، **أمن المعلومات والفساد الرقمي**، دار الفكر الجامعي، الإسكندرية، 2020.
10. فهد بن سعود العتيبي، **الأمن السيبراني وحماية المعلومات في مكافحة الفساد**، ط2، دار المعرفة للنشر، الرياض، 2023.
11. لورنس م. أوليفا، ترجمة محمد مراياتي، **أمن تقنية المعلومات: نصائح من خبراء المنظمة العربية**.
12. محمد حسن الخطيب، **الأمن السيبراني وأثره على الشفافية والحوكمة في المؤسسات**، ط1، دار النشر العربي، بيروت، 2023.

13. محمد بن عبد الله الراجحي، **الأمن السيبراني ودوره في تعزيز الشفافية والتعاون الدولي في مكافحة الفساد**، ط1، دار الفكر العربي، القاهرة، 2024.
14. محمد جمعة عبدو، **الفساد: أسبابه، ظواهره، آثاره والوقاية منه**، دار المطبوعات الوطنية.
15. خالد بن إبراهيم الفهد، **الشراكات الاستراتيجية في الأمن السيبراني: تعزيز الأمان من خلال التعاون**، ط1، دار المعرفة التقنية، دبي، 2023.

ثانيا: الرسائل الجامعية

1. حاجة عبد العالي، **الآليات القانونية لمكافحة الفساد الإداري في الجزائر**، أطروحة دكتوراه، جامعة محمد خيضر، بسكرة، 2012-2013.
2. إبراهيم الخثران عبد الكريم بن سعد، **واقع الإجراءات الأمنية المتخذة للحد من جرائم الفساد من وجهة نظر العاملين في أجهزة مكافحة الرشوة في المملكة العربية السعودية**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
3. بتة بدرة، **مكافحة الفساد في الجماعات المحلية في الجزائر**، مذكرة ماستر، 2020-2021.
4. بن علي يمينة، **دور المنظمات الدولية غير الحكومية في مكافحة الفساد (دراسة حالة منظمة الشفافية الدولية)**، مذكرة ماستر، جامعة محمد خيضر، بسكرة، 2018-2019.
5. بامحمد عبد القادر، وغزوز ياسين، **متطلبات تفعيل آليات مكافحة الفساد في الجزائر**، مذكرة ماستر، جامعة أحمد دراية، أدرار، 2019-2020.

ثالثا: المقالات العلمية والملتقيات والمحاضرات

1. بن دحمان حفيظة، "الإبلاغ الرقمي عن الفساد في الجزائر: بين النظرية والممارسة"، **مجلة الشفافية والمساءلة**، جامعة سطيف، 2022.
2. بن صالح زهير، "أثر أنظمة التدقيق الإلكتروني في تقليص الفساد الجمركي"، **مجلة الدراسات القانونية**، جامعة وهران، 2021.

3. جبوري، ندى إسماعيل، "حماية أمن أنظمة المعلومات: دراسة حالة مصرف الرافدين"، **مجلة تكريت للعلوم الإدارية والاقتصادية**، المجلد 7، العدد 2، بغداد، 2011.
4. حمدي نادية، "التوقيع الرقمي كأداة لحماية المعاملات الإدارية في الجزائر"، **المجلة الجزائرية للحوكمة الإلكترونية**، 2019.
5. خربط محمد، **محاضرات في مقياس مكافحة الفساد**، جامعة البليدة، 2020-2021.
6. زروقي غنية، "أثر السياسات الأمنية على مكافحة الفساد في المؤسسات الجزائرية"، **مجلة الدراسات القانونية والسياسية**، جامعة الجزائر 1، 2020.
7. الشاذلي ياسر، "الفساد الإداري في ظل التحول الرقمي"، **مجلة البحوث الإدارية**، جامعة القاهرة، 2018.
8. الشعري ليلى علي أحمد، "الفساد: مكافحته والوقاية منه (رؤية شرعية"(، **مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية**.
9. عزمي الشعبي، **الفساد السياسي في العالم العربي (دراسة حالة(**، تقرير إقليمي، 2014.
10. قارة ملاك، "آليات مكافحة الفساد في الجزائر بين النظرية والتطبيق"، الملتقى الوطني الأول حول الفساد وتأثيره على التنمية الاقتصادية، جامعة قسنطينة 2، 2019.
11. قروج مراد، "دور الأطر المرجعية الدولية في تحسين الأداء الرقمي الإداري: حالة ولاية الجزائر"، **المجلة الجزائرية للحكومة الإلكترونية**.
12. فوكراش زبيدة، **محاضرات مقياس أخلاقيات المهنة والفساد**، جامعة الشلف، 2019-2020.
13. محمد عباس نعمان الجبروني، "مفهوم الفساد في القرآن الكريم"، **مجلة كلية التربية الأساسية**، جامعة بابل، 2014.
14. موسى علي، "دور نظم المراقبة الرقمية في الحد من الفساد الإداري"، **مجلة العلوم الإدارية**، جامعة البليدة 2، 2020.

15. نوار حفيظ، "الحوكمة المعلوماتية كآلية لمكافحة الفساد في البيئة الرقمية"، **مجلة البحوث الاقتصادية والإدارية**، جامعة باتنة، 2021.
16. يوسف عبد عطية، "الفساد الإداري: المسببات والعلاج"، دراسة تطبيقية، جامعة غزة، 2011.
17. **محاضرات الفساد وأخلاقيات المهنة**، منشورة على الموقع الإلكتروني لكلية الحقوق والعلوم السياسية.

رابعا: النصوص القانونية

1. **القانون رقم 06-01** المؤرخ في 20 فيفري 2006، المتعلق بالوقاية من الفساد ومكافحته، المعدل والمتمم.

المراجع الأجنبية

1. Adam Shostack, **The Evolution of Information Security**, The Next Wave, Vol. 19, No. 2, 2012.
2. Jason Andress, **The Basics of Information Security**, 2nd Edition, Elsevier, USA, 2014.
3. Vladimir Aman Gnuan, **Concevoir la sécurité informatique en entreprise**, 2014.

فهرس المحتويات