ذكاء المؤسسة وأمن أنظمة المعلومات

الدكتور عزالدين شرّون- أ. عبد الحفيظ لقوي

- جامعة سكيكدة -

a.cherroune@uni-skikda.dz-azlekoui@gmail.com

ملخص.

باتت تنافسية المؤسسات ملخصة في قدرتها على تعبئة مهارات إستراتيجية جديدة كخلق المعرفة ونشرها سريعا عبر مسارات الإنتاج، القدرة على بناء الشبكات ودمجها والتنسيق فيما بينها باستخدام التكنولوجيا، التحكم في المعلومة وقدرة امتصاصها من قبل جميع الأطراف ذات الصلة.

كلما كانت مهارات المؤسسة الجديدة لامادية أكثر، كلما زادت حساسيتها وإمكانية إصابتها بالمخاطر المستحدثة التي تهدد اليوم الأصول المادية واللامادية للمؤسسات. الأمر الذي يلزم كل المسيرين على استباق، مواجهة بل مبادرة أصل المخطر من أجل حماية فعالة للذمة التكنولوجية والمعلوماتية.

الكلمات المفتاحية : الذكاء الاقتصادي، نظام المعلومات، الشبكات، الأصول اللامادية.

Abstract.

The competitiveness of companies is now based on their ability to mobilize new strategic skills, Such as the creation of knowledge (and its rapid diffusion in production processes), Such as the ability to foster networking (and its coordination through the use of technology), Such as information literacy (and its absorption capacity by all stakeholders).

More new business competence belongs to the intangible, becomes more sensitive and vulnerable. Faced with new types of threats today on tangible and intangible assets of enterprises, Any leader must anticipate, counter, or even retaliate In order to actively protect its technological and informational heritages.

Key worlds: economic intelligence, information's system, networks, intangible assets.

مقدمة.

يتطلب تعدد البنى التحتية الشمولية للمعلومات، المعرفة الدقيقة للإمكانات والكفاءات التي تتيحها حلول البرمجيات المتوفرة. فضلا عن كون هذه المشاريع تجمع غالبا العديد من الأدوات التي تمس المؤسسة في كليتها. مفاهيم التشغيل المتبادل لمختلف الحلول تثير تعقيدات تقنية أكيدة، كون الحلول المتاحة في لحظة ما يجب أن تندمج تماما مع نظام المعلومات القائم. من هنا ينشأ التساؤل الرئيس لهذه الدراسة:

أي دور للذكاء الاقتصادي للمؤسسة في حماية نظام معلوماتها؟

بحثا عن إجابة لهذا التساؤل نعتمد فرضية أن الذكاء الاقتصادي:

وإن كانت له دلالات هجومية فهو بمثابة جدار دفاعي متقدم ضد مخاطر نظام المعلومات.

وقد استخدمنا المنهج التحليلي استنتاجا واستقراء لمناقشة تفاصيل الدراسة التي اشتملت على محورين:

I- الذكاء الاقتصادي والمخاطر المعلوماتية؛

II- نظام المعلومات ومسيرة الذكاء الاقتصادي،

I- الذكاء الاقتصادي والمخاطر المعلوماتية.

يعبر الذكاء الاقتصادي عن سياسة اقتصادية عمومية في خدمة مصالح المؤسسات، سياسة أمن اقتصادي، تنافسية، وتأثير تقوم على تبادل المعلومات بين العمومي والخاص. لكن إدارة المخاطر المعلوماتية بالمؤسسة يقتضي أولا أخذ قدر من التحدي، فلا يمكن أن نحمي أو نراقب سوى ما نعي أننا نملكه أو بحاجة لتملكه.

تحديد مصادر المعلومات وتحسس تفاعلاتها يحتم على المسيرين تحليل مختلف مركبات نوع جديد من رأس المال يعرف برأس المال اللامادي [1] تأتي في مقدمتها أنظمة المعلومات وتشكل سيرو رة التنظيم جزء ا معتبرا منها سواء بالقياس إلى حجمها أو أهميتها الإستراتيجية وحتى أدائها. في اقتصاد شبكي، يبنى الذكاء الاقتصادي للمؤسسة على المعلومات وتلاقحها متجاوزة الاقتصاد الصناعي ولوجا إلى اقتصاد المعرفة [2]. الأمر الذي سيولد تحولات إن بخصوص التنظيم الداخلي للمؤسسة أوفي بيئتها الخارجية، نتيجة نزوعها لعمليات نقل المعرفة حتى تحافظ و/أو تدعم تنافسيتها عبر عمليات التملك والاندماج، التحالفات الإستراتيجية، عقود البحث والتطوير...

هذه الأنماط الوظيفية الجديدة وإن كانت تضفي حيوية أكثر وتزيد بنسبة كبيرة من الفعالية إلا أنها مصدر لتحديات أخرى، من حيث أن نقل المعرفة يولد مخاطر فقدان السيطرة المباشرة، التنازل عن بعض حقوق الملكية، التبعية لبعض مراكز التميز...، الأمر الذي يستدعي أشكال جديدة من التنسيق حول أنشطة التصور، الإنتاج والتسويق. لأجل ذلك يتعين على المسيرين وضع سيرورات لإثارة تفاعل مختلف المعارف الفردية حتى تولد معارف جماعية جديدة تسند عملية الابتكار بالمؤسسة (لاسيما منه التنظيمي)، لتنوير عملية اتخاذ القرار يراكم الذكاء الاقتصادي التحكم في تقنيات بلوغ ومعالجة المعلومات إلى إدارة المعارف لتشكيل قاعدة للذكاء الجماعي.

1- حسني عبد الرحمن الشيمي، **إدارة المعرفة**، الرأسم عرفية بديلا، ط 1، دار الفجر للنشر والتوزيع، القاهرة، 2009، ص:29.

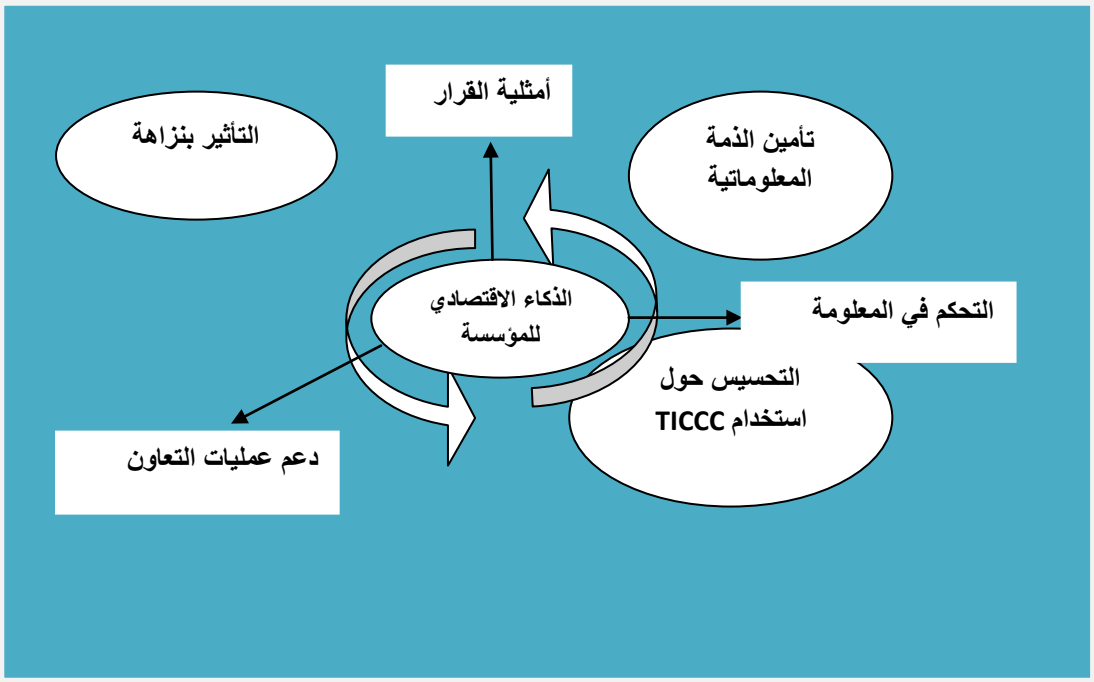
2- في مارس 2000 على إثر قمة لشبونة حدد الاتحاد الأوروبي التحول لأكبر اقتصاد تنافسية مبني على المعرفة كهدف لنهاية العشرية، بعد خمس سنوات صارت رؤية المؤسسات الأوروبية تصاغ حول التساؤل :هل مازلنا ضمن اقتصاد صناعي يحاول إدماج *TICCC أم دخلنا إلى براديغمات جديدة لاقتصاد المعرفة؟

* TICCC: Technologies de l'Information, de la Communication de la Connaissance et de la Coopération.

1-1- الذكاء الاقتصادي كثقافة تسييرية.

يقصد بالذكاء الاقتصادي للمؤسسة التحكم في المعلومة، ترقية التعاون لأمثلية القرار ما يحمل على القول أن المسألة تتعلق ابتداء بثقافة تسييرية بمعنى انقياد فردي ورغبة بالتفكير، و التعاون لأجل حسن الأداء الجماعي لذلك نجد له في بعده التنظيمي مجموعة خصائص تدعم عملية التنسيق يوجزها الشكل رقم (1).

الشكل رقم (1): خصائص الذكاء الاقتصادي للمؤسسة.



المصدر: تقرير CIGREF أكتوبر2000 بعنوان" إدارة المعارف"، متاح على الموقعwww.cigref.fr

يوضح الشكل أن الذكاء الاقتصادي للمؤسسة يرمي أساسا لتحكم المسير في المعلومات الإستراتيجية الضرورية لاتخاذ القرار والداعمة للعمل التعاوني،

أي تعاضد قيادتها لمجموع الأطراف الفاعلة بالمؤسسة وقدرتها على التأثير في بيئتها.[3]

I-2- ذكاء الإدارة.

في إطار المنافسة الدولية الراهنة تعد قدرة المؤسسة على السيطرة على المعلومة في الوقت الحرج بكل مكان وزمان لبناء وتطوير قاعدة معرفتها الإستراتيجية، الميزة التنافسية المستدامة الوحيدة. نجد (AFDIE)[4] تعتمد التعريف التالي: "...الذكاء الاقتصادي بالنسبة للمؤسسة أو المنظمة هو مجموع الوسائل المتراصة كنظام للإدارة بالمعرفة والمنتجة للمعلومة المفيدة لاتخاذ القرار ضمن منظور الكفاءة وإضافة أو خلق القيمة لكل الأطراف الفاعلة..."

II- المفهوم الحديث لكفاءة المؤسسة.

في مقابل التعقد المتنامي للبيئة الاقتصادية، التكنولوجية، الاجتماعية والسياسية بسبب ظهور فاعلين جدد ونظرا للتشابك والتبعية المتبادلة بين مختلف مستويات التأثير (محلي، وطني، إقليمي، دولي) الكفاءة الجديدة للمؤسسات تمارس وسط حقيقة اقتصادية لامادية أكثر فأكثر وهناك من يقول بأنها: "... ذكاء تطبيقي لمواقف ووضعيات يرتكز على معارف مكتسبة ويحولها بقوى أكبر من تزايد تنوع تلك الوضعيات..."[5].

وهكذا تتجلى للمسير فرصة أن يرى الحقيقة بشكل مختلف، المنظور الذي لم يكن معتمدا حتى بزغ فجر الألفية الثالثة أين بدأ الاقتصاد التقليدي القائم على الطاقة المادية بالتحول نحو اقتصاد جديد يقوم على الطاقة المعلوماتية الأمر الذي يحول ويعيد توزيع القيمة التي تخلقها المؤسسة[6].

3 - Eric Delbecque, Christian Harbulot**, la guerre économique**, que sais je ?,PUF, paris,2012,p 86.

4 -association française pour le développement de l'intelligence économique in **(Model D'intelligence Economique**, Economica, 2004), p41.

5- Philippe Zarifian, ***Objectif Compétence, pour une nouvelle logique***, Editions Liaisons, 1999, p27.

6- Rapport du CAE n0 71(2007),pp10-11.in Jean-pierre Allegret et Pascal Le Merrer, **Economie de la mondialisation opportunités et fractures**, Ed de boeck, Bruxelles, 2007, p307.

في ضوء هذا التحدي الجديد يتغير هدف المؤسسة تلقاء تحصيل وضمان ثلاث قدرات هي:

- القدرة على التأثير بنزاهة : من خلال الاتصال وأعمال الضغط (lobbying)؛

القدرة على تسيير واستغلال المعلومة : لإنتاج معرفة ذات طابع استراتيجي، تنظيمي وعملياتي ما يجعلها مفيدة ليس فقط للمسير بل لجميع الأطراف ذات الصلة من أعوان داخليين وخارجيين قد يساهمون في تنافسية المؤسسة والاقتصاد؛

القدرة على تأمين ذمتها المعلوماتية المشكلة: فضلا عن الأرضية التكنولوجية من المعلومات، العلم والمعرفة[7].

1- تأمين الذمة المعلوماتية.

تعد القدرة على خلق المعرفة الإستراتيجية انطلاقا من المعلومة إحدى نقاط القوة أو الضعف بالنسبة لأي مؤسسة، لكونها مدار رحى المنافسة الاقتصادية والاستراتيجيات غير المعلنة أو الخفية وحلقة الوصل الأساسية التي يتم عبرها بناء صورة المؤسسة و التأثير في بيئتها. إن التسيير الكفء للتهديدات و الفرص المرتبطة بهذا الأصل اللامادي يقتضي إيلاء أهمية خاصة للذمة المعلوماتية بالمؤسسة. التي قد تزيد في بحثها عن و/أو تقاسمها للمعلومات من احتمال قابلية تأثرها وهشاشتها، وعليه نلاحظ أن الخطر المعلوماتي ذو حدين: أولا رصد أو تحويل المعلومة الإستراتيجية، ثم احتمال كون المعلومة مؤكدة من عدمه ثانيا. الأمر الذي قد يغير أو يؤثر على صورة، سلوك وإستراتيجية المؤسسة.

ضمن هذا السياق الجديد، يفرض الذكاء الاقتصادي للمؤسسة تشغيل:

- إستراتيجية لتأمين المعلومة (أوجه تنظيمية وبشرية، أمن الأنظمة، القانون، اختيار الشركاء، مؤدوا الخدمات والموردين الثقة، التحكم في نشر بيانات المؤسسة على مواقع الشبكة العنكبوتية الدولية، التوثيق...)؛

7- Pierre Bardon et Thierry Libaert, **le lobbying**, DUNOD, paris, 2012, pp 16-17.

- سيرورة معلوماتية دفاعية فعالة (إدارة السمعة، مواجهة الإفقار المعلوماتي) مشاكل ضرب الاستقرار والشائعات تسيء إلى صورة علامة المؤسسة متى نقلت أو ضخمت عبر الانترنت. يمكن التصدي لهذه الهجمات بإستراتيجية اتصال وخطابات مناسبة، أما استباقها فيقتضي أن نكون في مستوى اكتشافها أي أن نتوفر على إمكانات مضادة للاستراتيجيات الهجومية؛

- عمل ضغطي للتأثير في ساحة الأحداث الخارجية على الصعيد المحلي، الإقليمي والدولي يسبق إبرام العقود والاتفاقيات.[8]

تنافسية المنظمة تابعة كما رأينا بشكل كبير لقدرتها على التسيير الفعال لسيرورات متقاطعة من أجل إدارة مثلى للمعرفة. تتطلب الارتكاز على قاعدة معلوماتية تشكل أنظمة المعلومات فيها حجر الزاوية.

2- نظام المعلومات و مسيرة الذكاء الاقتصادي.

"إن وضع مسيرة فعالة للذكاء الاقتصادي يجب أن يمر بالضرورة عبر تصور حول التنظيم الداخلي وأنظمة المعلومات". [9] إذ يمكن لأنظمة المعلومات أن تسرع تطور ثقافة تعاون جماعية حول المعلومات بفضل نجاعتها التقنية وتشعبها أفقيا. حيث أن تنوع المعلومات والمهارات والمعارف اللازمة لحل مشاكل أكثر فأكثر تعقدا يتطلب تنسيقا محكما بين مختلف الأطراف ذات الصلة، الأمر الذي صار متاحا بفضل تفاعل برمجيات متزايدة الفعالية وأجهزة مطردة القوة وكذا شبكات اتصالات عالية التدفقات.

3- تكييف نظام المعلومات مع سيرورة الذكاء الاقتصادي بالمؤسسة.

تسمح أنظمة المعلومات للمؤسسة بأن تشتغل بنمط أمثلي من خلال توفير أدوات التنسيق بين مهام مختلف وحدات المنظمة، لجميع المعنيين. ضرورة هذا التنسيق تلزم نظام المعلومات بتشغيل كل ما يسعه لحماية البيانات وأيضا

8Bernard Carayon, **A armes égales**, rapport remis au premier ministre français, juillet 2006, p17.

9 Enquête de L'IHEDN, in Michel-Henry Bouchet et Alice Guilhon le Fraper du Hellen, **intelligence économique et gestion des risques**, pearsoneducation, 2007, France, p 49.

استرجاع المعلومات، تخزينها، معالجتها ونشرها بحكمة، تأسيسا للعلم والمعرفة بالمؤسسة.

يعرف نظام المعلومات المكيف وسيرورة الذكاء الاقتصادي على أنه:

"مجموعة منظمة من الإجراءات تسمح بإعطاء المقررين في أية لحظة تمثيلا لمكانة المؤسسة في بيئتها وعلى سوقها. وتنتج المعلومة لمساعدة الأفراد في الوظائف التنفيذية، التسييرية ووظائف اتخاذ القرار"[10].

من هنا أصبح هذا الأصل اللامادي العامل الأساسي للمزايا التنافسية بالمؤسسة، كما يمكنه أن ينقلب وسيطا مريبا للتهديدات وأداة لا تقل أهمية للتبعية. حسن إدارة التهديدات والفرص المرتبطة بهذا الأصل تفرض إعطاء أهمية خاصة لحماية الذمة التكنولوجية للمؤسسة.

4- حماية الذمة التكنولوجية.

أمن أنظمة المعلومات بات خارج حدود المؤسسة بل تحد وطني استراتيجيا، سياسيا واقتصاديا.[11] سواء تعلق الأمر بالذمة الفكرية، التقنية، العلمية، المعلوماتية أو الاقتصادية فهي مسألة أصول إستراتيجية فعلية. الدفاع عنها صار قضية حيوية في بيئة شمولية أكثر فأكثر شراسة تنافسية[12]، لاسيما وأن هذه الذمم تشكل الركن الركين لأنظمة المعلومات المعلوماتية للمؤسسة.

المخاطر المرتبطة بالإعلام الآلي التي توشك أن تلحق خسائر بذمة المؤسسة تنقسم إلى ثلاث فئات:

- التهديدات المحدقة بالأصول الواجب حمايتها؛
- قابلية هذه الأصول للتأثر؛

10-Romagni Patrick et Wild Valérie, **L'intelligence économique au service de l'entreprise**, les presses du management 1998, p85.

11- Rapport du groupe « **intelligence économique et stratégie des entreprises** »,dir Henri Martre, commissariat générale du plan, la documentation française, paris, février 1994 , p6.

12-jacques fontanel et al, **globalisation économique et sécurité internationale (introduction à la géoéconomie)**, OPU-UPMF, algrer, 2005, p23.

- حساسية هذه الأصول، والمحددة تبعا لدرجة توفرها، سريتها ونزاهة المعطيات.

يمثل الخطر عموما على أنه ناتج هذه الفئات الثلاث.

أ- التهديدات.

تعزى ظاهرة اشتداد التهديدات لتنوعها، تشابكها وسرعة انتشارها بسبب اتصالها فيما بينها وتفاعلها المتزايد. وهي مصدر لأعمال عدوانية أو مخاطر غير متحكم فيها يمكن أن تسيء بشدة لمختلف مهن المؤسسة. والخسائر تتأرجح بين أعباء مالية، إسنادية أو ضغوطا على صورة المؤسسة. أما طبيعتها فقد تكون بشرية، مادية أو منطقية:

- بشرية: الاستعمال المفرط للأنترنت، غصب المراسلات، الملكية الفكرية، المعالجة غير المصرح بها للمعطيات الشخصية، الشائعات، الاعتداء على الهوية، التزوير...؛
- مادية: الكوارث (حرائق، فيضانات، تخريب، سرقة العتاد)، عيوب في الأنظمة أو سوء اشتغالها، مخاطر مرتبطة بادخال تكنولوجيات حديثة (nomadisme, Wi-Fi)...؛
- منطقية: أعمال عدوانية (داخلية، خارجية)، هجوم (virus, phishing, spasming)، سرقة/ضياع/مسح/إتلاف المعلومات، قلة معارف أو ضعف تحسيس الأعوان...

هذا وقد هدفت دراسات بعض الهيئات المختصة لمعرفة درجة الحساسية تبعا لنوعية التهديد فكانت النتائج كما يلي:[13]

- 100% أعمال عدوانية داخلية أو خارجية مرتبطة بالمستخدم؛
- 94% إصابات المعطيات الشخصية؛
- 87.5% هجومات كالفيروسات وغيرها تسمح بظهور خلل يسهل التسلل أو التلاعب بالمعطيات؛

13- CIGREF 2005 enquête sur la sécurité des SI

- 75% التسلل إلى نظام المعلومات يتيح بلوغا غير شرعي لمعطيات أو برامج مما يسبب سرقة، فقدان، حذف أو إتلاف المعطيات؛
- 74% الاستعمالات غير المطابقة للقانون كغصب أسرار المراسلات؛
- 68% عدم احترام قواعد الأرشفة؛
- 65% حراسة المحيط المعلوماتي؛
- 65% عدم احترام الملكية الفكرية؛
- 62.5% الكوارث، كالسرقة، الحرائق، الفيضانات... تتسبب في فقدان العتاد و/أو المعطيات.

ب- قابلية الإصابة.

الابتكارات التكنولوجية، تمدد للمؤسسة، تطور طرق العمل (الاتصال عن بعد، العمل التعاوني) يجبر نظام المعلومات على التأقلم لتسهيل العمل الشبكي بين جميع الأطراف ذات الصلة (الزبائن، الموردون، الآمرون، الشركاء، السلطات العمومية)[14].هذه التبعية المتبادلة ما بين المتدخلين جميعا تزيد من قابلية نظام المعلومات للإصابة. كما أن تعدد الاتصال البيني مصدرا لمخاطر جديدة بالنسبة للمؤسسة تضاف لتلك الناجمة عن انتشار الترحل الرقمي (nomadisme).

وعليه فمصادر قابلية الإصابة كثيرة وتتأتى من:[15]

- المؤسسة ذاتها: الإفصاح، معلومات غير مرتبة، الإخلال بمبدأ الأثر؛
- الفرد: عدم احترام التنظيمات، الجهل أو الاستهانة بالخطر، عدم توافق بعض الكفاءات مع الوظائف الحرجة، قلة الوعي أو الجهل بتهديدات اتصالات الأعمال، تعدد المتدخلين؛

14- Abdelhak Lamiri, **management de l'information**, redressement et mise a niveau des entreprises, 2eme ed, OPU, Alger 2003,pp 51-57 .
15- Michel-Henry Bouchet et Alice Guilhon le Fraper du Hellen, **op cité**, p52.

- البرمجيات: التعقيد المتزايد يكون غالبا مصدرا للأخطاء صعبة الاكتشاف، احتمال عيوب متعمدة أو ما يعرف بالأبواب الخلفية (back doors)؛
- شبكات الاتصال: مؤسسة متمددة، ترحال معلوماتي؛
- نظام البيئة المعلوماتية: المنافسة، التبعية لجهة مبتكرة...

ج- الحساسية.

تشمل الحساسية قابلية إصابة التكنولوجيات التي يقوم عليها نظام المعلومات ونجد فيها، أنظمة الاستغلال، البرامج، السيرورات، الأجهزة الطرفية... كما يمكن أن تستهدف أيضا مناطق أو نقاط معينة من نظام المعلومات، فترفع من المخاطر لاسيما ما تعلق بكشف أو تغيير المعطيات، مصادرها، توفرها، فسخ المعاملات المالية، التأكد من هوية المستخدمين، الالتفاف حول الرقابة على البلوغ.[16]

مهما يكن أصل العيب أو النقص في نظام المعلومات فإنه يمثل العديد من المخاطر التي يجب على المؤسسة التوقي ضدها وفق سياسة أمنية ملائمة.

د- حماية الذمة المعلوماتية.

- لتحديد سياسة أمثلية لأمن نظام المعلومات، يفترض الأخذ بعين الاعتبار لأبعاد الأمن والسلامة بشكل شامل، حيث يحددها ويقودها مسؤول عن أمن أنظمة المعلومات يسهر أيضا على حسن تطبيقها واحترامها وتدمج كذلك مدير أنظمة المعلومات، المدققين الداخليين، مديري الخطر والقانونيين؛
- إن وضع سياسة شاملة للأمن ولإدارة المخاطر يسمح للمؤسسة بتوقي المخاطر المحتمل أن تصيب كل أو جزء من ذمتها كما تضمن سلامة نظام معلوماتها؛[17]

16- André Corbillé Et Vincent Dumas, **business intelligence et portails**, le décisionnel dans un environnement web, Dunod, paris, 2006, pp10-13.
17- Abdelhak Lamiri, op cité, pp 67-69.

- مباشرتها بشكل مجمل ونظامي يجعلها تحسس جميع المستعملين بكامل المعضلات الأمنية: حماية وتأمين المعطيات، الشبكات المعلوماتية، أنظمة التشغيل، التطبيقات، الاتصالات والأمن المادي؛

- يتبع أمن أنظمة المعلومات السارية لدى المجموعات الكبرى تطور المخاطر، ويخضع بانتظام للتدقيق والتعديل، ما يسمح خصوصا بالتأكيد على تصنيع واندماج سيرورة الأمن (إدارة التصحيحات، الهويات، الأخذ بعين الاعتبار لخطر المورد...)، تدعيم التقارير المرتبطة بالمتطلبات التنظيمية الجديدة، تعميم تكوين وتحسيس المستعملين (المساءلة)؛

- مواءمة لثقافة المنظمة، هذه السياسة يجب أن تكون متجانسة توازن دوما بين استخدامات نظام المعلومات والقيود المطروحة، شاملة لكن انتقائية وموجهة، يفترض فيها أن تكون براغماتية، تشكيلية ومفهومة، كما ستكون أحسن إذا ما أرفقت بجانب تكويني مخصص لتحسيس المستعملين.

ه- السياسة الإجرائية.

عند الحديث عن السياسة الواجب إتباعها، لا يقتصر الأمر فقط على المنظور التقني (الهندسة)، بل نجدها تتجه نحو تسيير تنظيمي، منهجي وكذلك إدارة بشرية للخلل.

هناك مرحلتين لوضع سياسة شاملة لأمن أنظمة المعلومات:[18]

- قبلية: تحليل المخاطر، وضع ميثاق لاستعمال الموارد المعلوماتية، تصنيف المعلومات وإمكانية تتبعها...؛

- بعدية: التدقيق والرقابة الداخلية والخارجية، اختبارات الاختراق، التقارير ولوحات القيادة، التعديل، التكوين المتواصل...

المسيرة تتمثل في تحديد القواعد والإجراءات التنظيمية بهدف حماية ذمة المؤسسة. فهي تدمج على جميع المستويات تحسيسا وتكليفا بالمسؤولية لجميع مستعملي الموارد المعلوماتية. كما تمنحنا الموارد التكنولوجية يوما بعد يوم مزيدا

18- Michel-Henry Bouchet et Alice Guilhon le Fraper du Hellen, **op cité**, p53.

من الإمكانيات لكنها تنشئ مخاطر مرتبطة بالمستخدمين غير اللائقين، سلوكيات من شأنها توليد خلل في نظام المعلومات بما يهدد أمن ذمة المؤسسة.

من أجل حسن التحكم بهذه المخاطر المرتبطة بسوء استخدام التكنولوجيا يستحسن إكمال سياسة أمن المعلومات بقواعد أخلاقيات عمل خاصة بنظام المعلومات.[19]

قواعد لن يكون لها مدعى تهذيبي ولا بغرض تنميط السلوكيات، لكنها لإعطاء معالم المسيرة التي تنتظرها المؤسسة من مساهميها.

الخاتمة.

يكتسي توافق المؤسسة مع محيطها وتشغيل أشكال جديدة من التعاون العملي بُعدا استراتيجيا ذو أهمية أولى، رصد محثات (inducteurs) البيئة والاستجابة الملائمة لها، قراءة الأحداث واتخاذ القرارات المترتبة عنها. من شأنه أن يساعد المسيرين على أمثلية أداء شركاتهم من خلال خلق فرص إستراتيجية وتحديد مكامن الابتكار.

بفضل TICCC وخيمياء اللاماديات التي تنشرها في المؤسسة ولجنا عصر الاقتصاد بعد الصناعي الذي يطبعه تقييم عال للأصول غير الملموسة كالعلم و المعرفة و الذكاء الجمعي المشترك.

حيث على المؤسسة أن تزن وتقيس وتحسب لتسهر على حماية الرأسمال اللامادي تماما كما تفعله مع الرأسمال المادي الملموس.

استراتيجيات المفاضلة، تدفع بالمسيرين لاعتبار المعلومة موردا استراتيجيا مستقلا، مولدا للقيمة، وضمانا لاستمرارية المؤسسة.

بتغذيتها لجميع دواليب المؤسسة، تمثل المعلومات محركا وظيفيا. إذ في حالتها الخام حقول المعلومة واسعة وجد معتبرة، إنما التحكم بتدفقاتها في الوقت الحقيقي بكل مكان وزمان هو ما صار يشكل بالنسبة للمسيرين تحديا رئيسا للفعالية والتنافسية من خلال توليد معرفة إستراتيجية ذات منحى عملياتي.

19- Rapport CIGREF « ***déontologie de l'usage des SI*** »2006, p3.

في هذا السياق يمكن الحكم على نظام المعلومات بأنه: مورد حرج لبدل طاقات الابتكار، إدارة الأنشطة شبكيا وتحقيق هوية تنظيمية قوية.

تحدي حماية الذمة التكنولوجية والمعلوماتية للمؤسسة يعني التحكم في المخاطر المرتبطة بدورة المعلومات ضمن نسق المؤسسة المتمددة في بيئة جيوسياسية من عدم الأكادة.

الذكاء الاقتصادي للمؤسسة ليس غاية في حد ذاته، لكنه وسيلة لبلوغ الأهداف الحيوية من أمن، تنافسية وابتكار مستمر.