

## الدليل الرقمي كألية لإثبات الجرائم المعلوماتية The Guide Digital as a mechanism to proof information crimes



د. أمينة لميز<sup>1</sup>

<sup>1</sup> جامعة محمد بوقرة بومرداس، (الجزائر)

a.lemmiez@univ-boumerdes.dz

تاريخ النشر: 2023/06/15

تاريخ القبول للنشر: 2023/06/01

تاريخ الاستلام: 2023/12/26

**ملخص:** تعد الجرائم الإلكترونية واحدة من المخاطر التي تهدد المجتمعات في العصر الحديث مع تطور التكنولوجيا، وما لحقه من تطور في أساليب ارتكاب الجرائم، من خلال الاستخدام اللامشروع للوسائل الإلكترونية. لهذا كان لزاما على العدالة الجنائية التسلح بطرق إثبات تتمتع بنفس المواصفات التقنية والعلمية لإثبات هذه الجريمة فكان الدليل الجنائي الرقمي الوسيلة الوحيدة والاساسية لإثبات هذا النوع من الجرائم.

**الكلمات المفتاحية:** الدليل الرقمي، الاثبات، الجرائم المعلوماتية.

**Abstract:** Cybercrime is one of the risks that threaten societies in the modern era with the development Of technology, and the subsequent development in the methods of committing crimes ; Via from the illegal use of electronic means.

for that became an obligation to the justice It is a criminal offense to have evidence of scientific technical specification that has been presented to prove this crime ; that's why digital evidence is one of the most prominent developments of modern times in all legal systems ; of the fact that the digital evidence is an innovative and complex nature.

**Key words: : the Guide Digital; The Proof; Cyber Crime.**

\*د. لميز أمينة

## مقدّمة:

يعتبر اكتشاف دليل الإثبات الجنائي في الجرائم المعلوماتية أكثر صعوبة مقارنة بالأدلة المعتمدة في إثبات الجرائم التقليدية، نظراً لما يثيره هذا الدليل حول مدى إمكانية قبوله في الإثبات كدليل جنائي من جهة، وأتساع مجال أو مسرح الجريمة من جهة أخرى في تلك الجرائم العابرة للقارات والحدود الدولية، وكذا عدم ملائمة ومسيرة القوانين والأنظمة للقضايا المطروحة في هذا المجال.

الأمر الذي جعل مثل هذه الجرائم تهدد الدول ومؤسساتها العمومية والخاصة، خاصة أنه لا يوجد اتفاق عام بين الدول على مفهوم موحد للجرائم الإلكترونية بصفة عامة، وبالتالي عدم وجود توافق بين القوانين الجنائية وتلك المتعلقة بالجرائم الإلكترونية المعلوماتية، فهذه الجرائم جرائم سريعة التطور والانتشار، وجب أن تتظافر الجهود الوطنية والدولية لمواجهة هذه الجريمة، من خلال تطوير قوانينها وانظمتها لمواكبة هذه الجريمة الحديثة والخطيرة السريعة الانتشار وفق مجموعة من الإجراءات تتفاوت قيمتها القانونية من حيث الإثبات لذلك نخصص هذه الدراسة للإجراءات الأكثر دعماً وكفاية لمواجهة هذه الجرائم والمتمثلة أساساً في الدليل الرقمي كوسيلة أساسية وجد مهمة في اثبات الجريمة الإلكترونية، والدليل المعتمد من طرف كل الأنظمة الدولية لمواجهة ومكافحة هذه الجريمة.

نظراً لأهمية هذه الوسيلة في اثبات الجرائم المعلوماتية نطرح الإشكالية التالية: ما مدى كفاية ومواكبة الدليل الرقمي كوسيلة مستحدثة في إثبات الجرائم المعلوماتية؟  
نجيب عن هذه الإشكالية وفق محورين نعالج في المحور الأول مفهوم الدليل الرقمي كوسيلة مواكبة لإثبات الجرائم المعلوماتية.

أما المحور الثاني فنخصصه لمراحل مشروعية الدليل الرقمي أي المراحل التي يمر بها الدليل الرقمي حتى يكن مشروعاً من جهة ويمكننا من الوصول لإثبات الجريمة من جهة أخرى معتمدين في ذلك على المنهج الوصفي التحليلي لمختلف الأفكار والمفاهيم المطروحة والمتعلقة بهذا الموضوع.

## 1. مفهوم الدليل الرقمي كوسيلة مستحدثة في إثبات الجريمة الإلكترونية

أصبحت وسائل الإثبات الجنائي التقليدية اليوم تقف عاجزة عن مواجهة الجرائم الإلكترونية التي تنصب على المعلومات والبيانات المخزنة في نظم المعلومات والبرامج مما أدى إلى بروز ظاهرة جديدة وهي الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والإنترنت نتج عنها ما يسمى بالدليل الإلكتروني أو الدليل الرقمي لإثبات الجرائم الإلكترونية.

يعتبر هذا الدليل الرقمي الوسيلة الأساسية لإثبات هذا النوع من الجرائم، فهو عبارة عن مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال

والرسوم، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون (المطلب 2006، ص 88).

### 1.1. تعريف الدليل الرقمي:

الدليل الرقمي لغة هو المرشد وما يستند عليه اما قانونا فهو إقامة البيئة والبرهان والحجة على المجرم المعلوماتي امام القضاء بالاستناد للقواعد القانونية في حال وجود نزاع بين الخصوم وهذا تعريف عام للدليل الجنائي، يتشابه مع الدليل الرقمي لكن يختلف عنه من حيث المضمون (محمودي 2017، ص 911).

ويعرف الدليل الرقمي هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات او نبضات مغناطيسية او كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات و تكنولوجيا وهي مكون رقمي لتقديم معلومات في اشكال متنوعة مثل النصوص المكتوبة او الصور او الأصوات او الاشكال والرسوم وذلك من اجل اعتماده امام أجهزة انفاذ وتطبيق القانون (يوسف 2009، ص 29)، ويعرفه الدكتور عمر محمد أبو بكر بن يونس على أنه: "الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة" (محمد 2004، ص 699)، فهو بذلك يعتبر طريقة خاصة لإظهار الحقيقة.

يعد الدليل الرقمي بمثابة جسم الجريمة المعلوماتية هو الذي يقود المحقق إلى الجريمة، حيث يستعين به المحقق بتقنية المعالجة الآلية للبيانات، والذي يؤدي بقاضي الموضوع إلى اقتناعه بثبوت ارتكاب الجريمة من شخص ما، خاصة وان هذا الدليل يتجاوب مع التطور الحاصل بسرعة فائقة يتميز بالسرعة والدكاء، حيث يأخذ الدليل الرقمي عدة تقسيمات:

\* أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكتها،

\* أدلة خاصة ببروتوكولات تبادل ونقل المعلومات بين أجهزة الشبكة العالمية للمعلومات، لسجلات المحفوظة في الحاسب الآلي وتشمل الوثائق والملفات المكتوبة والمحفوظة كالبريد الإلكتروني.

\* السجلات التي تم إنشاؤها وإعدادها بواسطة الحاسوب .... (المطلب 2006، ص 88).

### 2.1. خصائص الدليل الرقمي

على اعتبار ان الدليل الرقمي وليد البيئة الالكترونية الحديثة وينتمي لعالم افتراضي ويرتبط بالجريمة الالكترونية التي تختلف عن الجريمة التقليدية، الامر جعله يتميز بخصائص تختلف عن الأدلة الأخرى تتمثل في مايلي:

أ/ الدليل الرقمي دليل علمي وتقني: الدليل الرقمي هو الواقعة التي تنبئ عن وقوع جريمة أو عمل غير مشروع في العالم الافتراضي، فهذه الخاصية تفيد أنه ال يمكن الحصول على الدليل الرقمي أو الاطلاع على فحواه الا باستخدام الوسائل العلمية والتقنية أي تبني عملية البحث والتحري حول هذا الدليل وفق أسس علمية بطريقة تجعله يتجاوب مع الحقيقة بصفة كلية، ونفس الامر فيما يتعلق بحفظ

هذا الدليل وفق أساليب علمية مما يجعل تحرير المحاضر يختلف عن المحاضر الذي يبني على شهادة الشهود مثلا، فالمحاضر بالدليل العلمي يعني وجوب توافر طريقة عملية متوافقة مع ظاهرة الدليل العلمي أثناء تحريره، فمن غير المنطقي أن يتخذ صورة المحاضر التقليدي (عزت 2010، ص 648). وعليه فالدليل الرقمي ليس كالدليل العادي ففي الدليل الرقمي يتم التعامل مع نبضات الكترونية تقنية محضة تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه، لذلك فكل ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي.

ب/ الدليل الرقمي دليل يصعب التخلص منه: هذه الخاصية أو الميزة من أهم خصائص الدليل الإلكتروني، فالأوراق والاشربة المسجلة التي تكون كأدلة تقليدية يمكن حرقها وتمزيقها، كما أنه من المستطاع التخلص من بصمات الأصابع بمسحها من موضعها، أما بالنسبة للأدلة الإلكترونية فإن الأمر مختلف، حيث أنه يمكن استرجاعها بعد محوها وإصلاحها بعد تلفها، و بعد إخفائها مما يؤدي لصعوبة التخلص منه فكل هذا يشكل صعوبة إخفاء الجاني لجريمته، أو التخفي عن أعين العدالة أو غيرها بعد ما يتمكن رجال البحث والتحقيق الجنائي من اكتشاف الجريمة (أمينة 2015، ص 11).

ج/ الدليل الرقمي دليل متنوع ومتطور: مصطلح الدليل الإلكتروني يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقميا، أما أن يكون متنوعا كأن يكون في شكل صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الإلكتروني (عزت 2010، ص 652/651).

تتكون الأدلة الرقمية من بيانات و معلومات ذات بيئة إلكترونية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلب ادراكها الاستعانة بالأجهزة والمعدات والأدوات الآلية واستخدام نظم برمجية حاسوبية (مراد 2019، ص 208) أي انها ادلة رقمية خاصة بالشبكة الدولية للمعلومات "الانترنت" (المسماري 2007، ص 14).

\* يعد الدليل الرقمي من طبيعة تقنية وهذا ما يميزه عن الدليل التقليدي، فالدليل الرقمي ينتج نبضات رقمية تكمن قيمتها في إمكانية التعامل مع القطع الصلبة التي يتكون منها الحاسب الآلي مهما كان نوعه.

\* إمكانية توظيف نشاط الجاني لمحو أو إزالة الدليل من الحاسب الآلي كدليل إدانة ضده، لأن فعل الجاني بمحو الدليل يتم تسجيله في الحاسوب و، الذي يمكن الحصول عليه لاحقا كدليل للإدانة.

إذن نلاحظ من خلال هذه الخصائص ان الدليل الرقمي هو مفهوم يحتوي التطور والتنوع، ذلك لأن هذا مصطلح يتضمن كافة أشكال وأنواع البيانات الرقمية التي يمكن تداولها رقميا، بحيث يكون بين هذه البيانات والجريمة رابطة أو علاقة من نوع ما تتصل بالضحية أو المجني عليه على النحو الذي يحقق هذه الرابطة .

لكن في نفس الوقت ورغم الخصائص المميزة لهذا الدليل إلا أنه هو الآخر يواجه عدة صعوبات في الحصول عليه تتمثل هذه الصعوبات أو العراقيل في عراقيل تتعلق بالدليل في حد ذاته وأخرى تتعلق بالجاني، أهم هذه العراقيل نذكر على سبيل المثال:

\* الدليل الرقمي دليل غير مرئي أي أن بياناته لا تفصح عن شخصية معينة كما أن هذه البيانات مسجلة بكثافة وبصورة مرمزة على دعائم ضوئية وممغنطة كما يمكن محوها وتعديلها دون ترك أي أثر في فترة زمنية يسيرة فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها وبالتالي تنصله من مسؤولية هذا الفعل (البركة، 2019، ص 269).

\* استخلاص الأدلة يعد بمثابة تحدي لرجال الأمن والتفتيش والتحقيق، فرجل الأمن مثلاً غير المتخصص والذي انحصرت معلوماته في جرائم قانون العقوبات بصورة تقليدية من قتل وضرب وسرقة لن يكون قادراً على التعامل مع الجريمة المعلوماتية التي تقع بطريقة تقنية لذلك فغالبية الجرائم الإلكترونية تكشف مصادفة وليس بطريق الإبلاغ عنها (خريبط، 2016، ص 09)، ناهيك عن ضرورة توفر الإمكانيات التقنية اللازمة والكفاءات المتخصصة في هذا المجال للتحقيق في الجرائم المعلوماتية.

\* حماية الدليل الرقمي بوسائل فنية تتمثل أساساً في كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والإطلاع عليها أو استنساخها (الفيل، 2012، ص 80).

\* إضافة إلى سلوكيات الجاني المتمثل في تشفير تلك الملفات أو البيانات الإلكترونية التي تتضمن محتوى غير مشروع بغية منع الغير من الإطلاع عليها واكتشافها وهو ما يشكل قبة كبيرة أمام إثبات الأدلة الرقمية.

\* كما أن المجني عليه غالباً ما يمتنع عن التبليغ خاصة إذا كان المجني عليه مؤسسة كبيرة كالبنوك التي تفضل في كثير من الأحيان عدم التبليغ عن الإصابة بفيروس حتى لا تهتز ثقة المتعاملين معها (البركة، 2019، ص 247).

## 2. مراحل مشروعية الدليل الرقمي

يعد الإثبات من التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم المعلوماتية، وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به الكثير من الصعاب، مما يتطلب الكثير من الجهد والخبرة الفنية، حيث تستدعي في المقام الأول اكتشاف الجريمة الإلكترونية ومحلها وبيئتها ثم الإبلاغ عنها، واخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للمواقع، وذلك للبحث عن الدليل الرقمي الإلكتروني بالطرق التقنية والفنية، فالطرق التقليدية في استخلاص الأدلة يصاحبها الكثير من المشكلات العملية، ويكشف التحليل العميق لهذه الطرق أن

هناك بعض الخطوات يمكن إلغاؤها باستخدام نظام يقوم على تكنولوجيا المعلومات والاتصالات ووعليه حتى يكون الدليل الرقمي مشروعاً لا بد ان يمر بعدة مراحل تتمثل في كل من:

## 1.2. مرحلتى التحريز والتحليل:

أولاً نبدأ بمرحلة التحريز حيث أنه أثناء هذه المرحلة يكون المحقق أو الخبير في وضع لا يعرف أي نوع من البيانات يمكن من خلالها الحصول على دليل جنائي رقمي، وعليه الحفاظ على النظام الرقمي وكامل القيم الرقمية ليتم تحديد الضرورية منها لاستخلاص الدليل لاحقاً، وكذلك يستلزم نسخ جميع البيانات المخزنة داخل الحاسب الآلي موضوع الجريمة إلى الحاسب الخاص بالمختبر الجنائي الرقمي للاعتماد عليها، بالإضافة إلى نسخ البيانات المخزنة داخل جهاز الحاسب الآلي المشكوك فيه، ثم يقدم الدليل ويعرض على المحقق للاستعانة بها في عملية الإثبات (محمودي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية جوان 2017، ص 903).

أما الأمر المهم جداً في مرحلة التحليل هو وجوب قيام الفحص والتحليل على نسخ مطابقة الأصل لعدم تغيير خصائص الملفات، حيث يتم الحفاظ بالنسخة الأصلية المضبوطة من أجل التحقيق والتدقيق على أن البيانات الموجودة مطابقة للأصل ولم يطرأ عليها أي تغيير أو حذف.

يهدف من وراء قيام عملية الفحص والتحليل إلى استنباط ثلاثة أنواع من الأدلة:

\* دليل الإدانة، ويعد الدليل المؤكد والمستند إلى وجود فكرة معينة على ارتكاب وإسناد الجريمة محل التحقيق.

\* دليل البراءة ويعتبر الدليل الذي يخالف فكرة ارتكاب الجريمة موضوع التحقيق .

\* دليل محايد هو الدليل غير المرتبط لا بالإدانة ولا بالبراءة، بل يستعان به في إثبات أنه لم يطرأ أي تعديل أو تغيير في النظام الرقمي للحاسب الآلي لاستبعاد استخدام محتوياته أو الاستعانة به كدليل (الحميد 2006، ص 90).

## 2.2. مرحلتى العرض والقبول:

مرحلة العرض يتم من خلالها تقديم وعرض النتائج التي تم التوصل إليها عن طريق التحقيقات والفحص والتحليل الفني إلى جهة المحكمة المختصة، ويطبق على عملية هذه المرحلة النظام الجنائي المطبق في تلك الدولة ويستلزم الأمر موثوقية الأدلة الجنائية الرقمية لضمان مصداقيتها، حيث أنه يمكن توثيق الأدلة الجنائية الرقمية بالعديد من الوسائل المختلفة منها التصوير الفوتوغرافي، التصوير بالفيديو والقيام بنسخ الملفات المخزنة في الأقراص أو في الحاسب الآلي.

كما يستوجب أيضا تدوين التاريخ والوقت وتوقيع الشخص الذي قام بإجراء الحفظ عند حفظ الأدلة الرقمية، بالإضافة إلى اسم ونوع نظام التشغيل والمعلومات المسجلة في الملف المحفوظ وقسم البرنامج أو الأوامر التي استعملت في إعداد النسخ.

أما مرحلة قبول الأدلة الجنائية الرقمية في الإثبات موقوف إلى مدى توافر هذا الدليل في النصوص القانونية بالنسبة لنظام الإثبات المحدد، وإلى مدى اقتناع القاضي الجنائي بالدليل الرقمي بالنسبة لنظام الأدلة الإقناعية (الحميد 2006، ص 87-88).

وحتى يقتنع القاضي بالدليل الرقمي لابد أن تتوفر شروط تتمثل أساسا في:

لابد أن تكون هذه الأدلة يقينية تقترب للحقيقة الواقعية.

طبقا للمادة 212 من قانون الإجراءات الجزائية فإنه لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له أثناء المرافعات أو التي حصلت فيها المناقشة حضوريا، أي أنه يتم معاينة هذا الدليل شفويا.

يجب أن يكون الدليل الرقمي مشروعا أي أن طريقة الحصول على الدليل الرقمي تكون وفق الإجراءات المحددة بموجب القانون وإلا كان باطلا (محمودي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية جوان 2017، ص 919-920).

### الخاتمة:

من خلال هذه الورقة البحثية توصلنا إلى أن الجريمة الإلكترونية تتمتع بطبيعة قانونية مغايرة للجرائم التقليدية من جهة، كون أن أساليب مواجهة وإثبات الجريمة بالطريقة التقليدية لم تعد مجدية اليوم أمام هذه الجرائم المعلوماتية، لا سيما المتعلقة منها بخصوصية الدليل الإلكتروني وخصوصية التحقيق، و المتمثلة في عدم ظهور الدليل الإلكتروني وسهولة محوه أو تدميره، وصعوبة التحري عنه في كشف غموض الجريمة والوصول إليه، وكذا ضعف التعاون الدولي في مكافحة هذا النوع من الجرائم.

رغم التطور المذهل للتشريعات الجنائية العالمية، ولكنها بقيت عاجزة عن مواجهة الجرائم الإلكترونية، ونتيجة لخصوصيتها وطابعها غير الملموس سيتعذر تطبيق النصوص التقليدية لقانون العقوبات، وأية محاولة لتحميلها بما لا يطاق قد تصطدم بمبدأ الشرعية، لذا بدأ المشرعون ينتهون إلى ضرورة محاصرة الإجرام المعلوماتي بقواعد جديدة ونصوص تتلاءم مع طبيعتها الخاص في مقدمتها الدليل الرقمي كوسيلة جوهرية وجد مهمة في الوصول الى اثبات الجريمة الإلكترونية وتحديد الجاني المعلوماتي.

من خلال ما تم طرحه نوصي بضرورة عولمة القانون الجنائي المعلوماتي كون ان الجريمة المعلوماتية جريمة عابرة للحدود من جهة وترتكب في عالم افتراضي لا بد ان تحكمه قوانين عالمية مواكبة للتطورات التكنولوجية الحديثة والمستحدثة، كما ان هذا يؤدي الى ضرورة التعاون الدولي في مكافحة هذه الجريمة والعمل على تطوير أدلة إثباتها، وتعزيز التعاون والتنسيق بين مختلف الدول والمؤسسات الدولية المعنية بمكافحة الجريمة الالكترونية عن طريق عقد اتفاقيات ثنائية وجماعية ذات علاقة بالأدلة الإلكترونية والأنظمة المشتركة.

### قائمة المراجع والإحالات:

- عبد الله مدوح عبد الحميد، (2006)، البحث والتحقيق الجنائي الرقمي في الكمبيوتر والانترنت، دار الكتب القانونية، مصر.
- المسماوي محمد سيف سعيد، فرغلي عبد الناصر، (2007)، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية دراسة تطبيقية مقارنة. المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي.
- عبيد المطلب، ممدوح عبد الحميد، (2006)، البحث والتحقيق الجنائي الرقمي في الكمبيوتر والانترنت، دار الكتب القانونية، مصر.
- محمودي نور الهدى، (2017)، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد الحادي عشر.
- مراد فلاك، (2019)، آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الالكترونية، مجلة الفكر القانوني والسياسي، العدد الخامس.
- يوسف أمير فرج، (2009)، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية.
- عمر محمد ابو بكر بن يونس، (2004)، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين الشمس.
- أمينة هلال، (2015)، الإثبات الجنائي بالدليل الإلكتروني، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي. كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة.
- عزت فتحي محمد أنور، (2010)، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع.



- الطيب البركة، (2019)، إشكالية الاثبات في الجرائم الالكترونية، مجلة افاق علمية، المجلد 11، العدد 01.
- جاسم خريبط خلف، (2013)، مقال بعنوان الدليل الجنائي في الجريمة المعلوماتية، مجلة لقانون للدراسات والبحوث القانونية، جامعة ذقار.
- علي عدنان الفيل، (1949)، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية- دراسة مقارنة، ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الإسكندرية.