ميزان

إطار عمل كمّي للامتثال الأخلاقي
في التحقيقات الاستخباراتية مفتوحة المصدر

عمر ال سميح

مسودة بحثية

github.com/gqnxx/mizan-ethics

الملخص

تعاني التحقيقات الاستخباراتية مفتوحة المصدر اليوم من فشلين جوهريين موثقين. الأول هو **تأثير المراقب**، حيث يترك فعل التحقيق في هوية رقمية آثاراً قد تُنبّه الهدف، أو تُفسد مسار التحقيق، أو تُلوّث البيئة الرقمية المحيطة. والثاني هو **تسريب البيانات المجاورة**، حيث تنكشف بيانات أشخاص غير مستهدفين — كأفراد الأسرة والزملاء والمعارف — عندما يفتقر التحقيق إلى حدود أخلاقية رسمية ومنهجية قابلة للقياس.

رغم تنامي الوعي بهذه الإشكاليات، لا يزال الميدان يعتمد على الاجتهاد الشخصي وأفضل الممارسات النوعية التي لا تقدم أي معيار كمّي قابل للمراجعة أو إعادة الإنتاج. يطرح هذا البحث **بروتوكول ميزان**، وهو إطار عمل رسمي صُمّم لقياس نصف قطر التأثير الرقمي وتقليله لأي عملية تحقيق استخباراتي، من خلال نموذج تركيب أدلة معدوم التلامس ومعادلة رياضية استكشافية لتقييم المخاطر الأخلاقية.

الكلمات المفتاحية: *الاستخبارات مفتوحة المصدر، أخلاقيات التحقيقات الرقمية، تأثير المراقب، تسريب البيانات المجاورة، حماية الخصوصية، سلسلة العهدة الرقمية، نظام حماية البيانات الشخصية*

١. المقدمة: أزمة الاستمرارية الأخلاقية

مع تعاظم ترابط البصمات الرقمية واستمراريتها، ذاب الخط الفاصل بين ما يُعدّ بيانات متاحة للعموم وما يُعدّ حياة خاصة ذوباً فعلياً. فنشاط الفرد على منصات التواصل الاجتماعي، وبيانات موقعه الجغرافي، ومعاملاته الإلكترونية، وشبكة علاقاته المهنية والشخصية — كل ذلك يُشكّل نسيجاً رقمياً مترابطاً يكشف ما هو أعمق بكثير من أي نقطة بيانات منفردة، بمجرد النفاذ إلى طرف منه.

أخلاقيات الاستخبارات مفتوحة المصدر في صيغتها التقليدية تعتمد على التقدير الذاتي: هل هذه البيانات عامة؟ هل مسوّغي كافٍ؟ هذه التساؤلات، على أهميتها، تفتقر إلى الصرامة الكمّية ولا يمكن مراجعتها أو إعادة إنتاجها أو توحيدها عبر الفرق العاملة. بروتوكول ميزان يسعى إلى الانتقال من التقييم الذاتي إلى **الشهادة الأخلاقية الموثّقة**، حيث يُلزَم كل عنصر بيانات في التحقيق بحمل مصدر موثّق ودرجة تأثير محسوبة حسابياً قبل إدراجه في حافظة الأدلة.

١.١ تأثير المراقب في التحقيقات الاستخباراتية الرقمية

تأثير المراقب ليس افتراضاً نظرياً. إنه ظاهرة ميدانية قابلة للقياس والرصد، تُقوّض التحقيقات الاستخباراتية الرقمية بشكل يومي، وتتجلى في المحاور التالية:

- **أنظمة الإشعارات في المنصات الرقمية:** تعرض المنصات المهنية قوائم بمن اطّلع على الملف الشخصي، وتُظهر تطبيقات المراسلة الفورية تأكيدات القراءة، وتُسجّل شبكات التواصل مواقع ولحظات الوصول. مجرد استعراض الملف الرقمي للهدف قد يُولّد تنبيهاً يدفعه إلى تغيير سلوكه أو إتلاف الأدلة أو تعزيز إجراءاته الأمنية.

- **الرصد السلوكي الآلي:** تنشر المنصات الكبرى منظومات تعلّم آلي ترصد أنماط سلوك المستخدمين. التصفّح المنهجي والمشاهدة المفرطة للملفات الشخصية وأنماط طلبات الارتباط المتسارعة وأوقات الولوج غير المعتادة — كلها تُلتقط آلياً وقد تُجمّد حساب المحقق أو تُنبّه إدارة المنصة.

- **البصمة الرقمية للمحقق:** حتى عند استخدام الشبكات الافتراضية الخاصة، يترك المحقق آثاراً يمكن تعقّبها عبر تسريبات بروتوكولات الاتصال الفوري، وبصمة المتصفح الفريدة، وسجلات ملفات الارتباط، وسلسلة وكيل المستخدم.

- **تلويث الأدلة السلوكي:** حين يُدرك الهدف وجود مراقبة — حتى لا شعورياً — يتبدّل سلوكه الرقمي. تُمحى المنشورات، وتُغلق الحسابات، وينتقل التواصل إلى قنوات مشفّرة. وبذلك يكون التحقيق قد أتلف الأدلة التي سعى لاستخلاصها.

١.٢ تسريب البيانات المجاورة: الضرر الجانبي غير المرئي

يُمثّل انكشاف غير المستهدفين الجانب الأشدّ خطورة أخلاقياً في التحقيقات الرقمية غير المنهجية. فحين يرسم المحقق خريطة الشبكة الاجتماعية للهدف، فإنه ينفذ حتماً إلى بيانات أفراد لا صلة لهم بالقضية:

- **الانكشاف الأسري:** قد تُلتقط الملفات الشخصية والصور وبيانات المواقع الخاصة بزوج الهدف أو أبنائه أو والديه، وتُخزّن في حافظة التحقيق دون سند أخلاقي أو قانوني.
- **التلوث المهني:** قد يُوسم الزملاء وشركاء العمل بوصفهم أشخاصاً محل اهتمام، لا لسبب سوى قربهم الرقمي من الهدف.
- **مخاطر التعريف الخاطئ:** أفضى التعريف الخاطئ في تحقيقات مفتوحة إلى تعرّض أبرياء للتشهير والمضايقة والتهديد المباشر. هذا نمط موثّق بعواقب واقعية مؤكدة.

لا يُقدّم أي إطار عمل قائم طريقة كمّية لقياس هذا الانكشاف الجانبي أو الحدّ منه. بروتوكول ميزان يسدّ هذه الثغرة مباشرة.

٢. حساب نصف قطر التأثير

المساهمة الجوهرية لهذا الإطار هي **حساب نصف قطر التأثير**، وهو معادلة استكشافية لتحديد درجة المخاطر الأخلاقية لأي مسار تحقيقي قبل الشروع في تنفيذه.

٢.١ المعادلة

تُعرّف درجة المخاطر الأخلاقية بالصيغة التالية:

$$ERS = \Phi(S, A, E)$$

حيث تُحسب من ثلاثة متغيرات مستقلة:

المتغير	الوصف
الحساسية (ح)	القيمة الخصوصية المتأصلة في البيانات المُراد النفاذ إليها. تتراوح من محتوى عام بالكامل إلى بيانات بالغة الحساسية كسجلات الموقع الجغرافي المسرّبة. تُقاس على سلّم من صفر إلى واحد.
القرب (ق)	درجة الفصل بين صاحب البيانات والهدف الأساسي. القيمة صفر تعني الهدف ذاته. القيمة واحد تشير إلى اتصال من الدرجة الأولى. كلما ارتفعت القيمة، تعاظم التبرير المطلوب أخلاقياً.

الاضطراب (ض)	مقدار الأثر الذي يُحدثه أسلوب الجمع في البيئة الرقمية للهدف. الأساليب السلبية كاستعراض النسخ المؤرشفة تحمل اضطراباً منخفضاً. الأساليب النشطة تحمل اضطراباً مرتفعاً.

٢.٢ الحدّ الأخلاقي والمنطق القراري

تُقبل خطوة التحقيق فقط حين تقع درجة المخاطر الأخلاقية دون الحدّ الأخلاقي المعتمد. هذا الحدّ قابل للتعديل وفقاً لسياق التحقيق: إنفاذ القانون يتحمل مستوى مخاطر مختلفاً عن الأمن المؤسسي أو التحقيق الصحفي أو البحث الأكاديمي. تحدّد المؤسسة المسؤولة هذا الحدّ وتوثّقه ضمن سياسة التحقيق.

٢.٣ التطبيق العملي

قبل أي خطوة جمع بيانات، يحسب المحقق أو الأداة الآلية درجة المخاطر الأخلاقية. إذا تجاوزت الدرجة الحدّ المعتمد، تُحظر الخطوة ويتعين إما استبدالها بأسلوب أقل اضطراباً، أو تصعيدها لمراجعة أخلاقية رسمية مع توثيق كتابي للمسوّغ. ينشأ عن ذلك مسار قرارات قابل للمراجعة المستقلة لكل عنصر أدلة يُجمع.

٣. تركيب الأدلة بالحد الأدنى من التداخل

الركيزة الثانية لبروتوكول ميزان هي منهجية تركيب الأدلة بالحد الأدنى من التداخل، المصممة لجمع الأدلة مع تقليل التفاعل المباشر مع البيئة الرقمية للهدف أو إلغائه كلياً.

٣.١ المبادئ التشغيلية

- **أولوية النسخ المؤرشفة:** يُفضّل دائماً الرجوع إلى النسخ المخزّنة مؤقتاً أو المؤرشفة بدلاً من الوصول المباشر للخادم الأصلي.
- **التركيب عبر طبقات الإخفاء:** حين يكون الوصول المباشر حتمياً، يُمرّر عبر طبقات إخفاء هوية متعددة تمحو البصمات الرقمية.
- **الفصل الزمني:** تجنّب النفاذ إلى نقاط بيانات مترابطة خلال نوافذ زمنية ضيقة.
- **التحقق من انعدام الأثر:** كل أسلوب جمع يُختبر في بيئة رقابية محكومة للتأكد من خلوه من أي إشارة قابلة للكشف.

٣.٢ متطلبات الأمن التشغيلي

- بيئات تحقيق مخصصة عبر أجهزة افتراضية معزولة بأنظمة تشغيل مصمّمة للخصوصية
- شبكات افتراضية خاصة بسياسة عدم الاحتفاظ بالسجلات مع تقارير تدقيق مستقلة
- عشوائية بصمة المتصفح عبر إعدادات مخصصة لكل جلسة
- تقسيم صارم للهويات الرقمية أثناء عمليات التحقيق
- تطهير البيانات الوصفية لجميع الملفات المجمعة

٤. إثبات السلوك الأخلاقي

كل عنصر أدلة يُجمع في إطار بروتوكول ميزان يجب أن يحمل توقيع **إثبات السلوك الأخلاقي**، وهو سلسلة عهدة رقمية كاملة تربط كل دليل بمصدره وأسلوب جمعه ومسوّغه الأخلاقي:

المكوّن	الوصف
مسار المصدر	العنوان الرقمي الدقيق أو الواجهة البرمجية التي استُخرج منها الدليل. يجب أن يكفي للمراجعة المستقلة.
أسلوب الوصول	الأداة وإعدادات المتصفح وتكوين الشبكة والطوابع الزمنية. يُمكّن من التحقق الجنائي.
درجة المخاطر الأخلاقية	الدرجة المحسوبة لحظة الجمع مع الحدّ المُطبّق. يثبت أن التقييم سبق الجمع.
منطق المسوّغ	تبرير رسمي مكتوب لسبب النفاذ إلى البيانات دون موافقة صاحبها.
تجزئة السلامة	بصمة تشفيرية تُحسب لحظة الالتقاط. أي تعديل مهما صغر يُبطلها.

٥. الحساسية الإقليمية وسياق المجتمعات مرتفعة الترابط

صُمّمت غالبية أطر عمل أخلاقيات الاستخبارات مفتوحة المصدر وفق نموذج الثقافة الرقمية الغربية، حيث الشبكات الاجتماعية منتشرة ومتفرقة، والبنى الأسرية نووية محدودة، ومعايير الخصوصية فردية بالدرجة الأولى. هذه الافتراضات تنهار حين تُطبّق على ثقافات مرتفعة الترابط الاجتماعي. يتناول هذا القسم المملكة العربية السعودية ومنطقة الخليج بوصفهما نموذجاً رئيسياً.

٥.١ كثافة الشبكات الأسرية

في المملكة العربية السعودية ومنطقة الخليج، قد يكون للفرد الواحد أربعون إلى ثمانون ابن عم، يشتركون جميعاً في اسم الأسرة، ويقطن كثير منهم في المدينة ذاتها. ما يُعدّ اتصالاً من الدرجة الثانية في السياق الغربي هو عملياً اتصال من الدرجة الأولى في السياق الخليجي. التحقيق في فرد واحد ينشئ موجة تأثير قادرة على كشف سلالة أسرية بأكملها. يعالج البروتوكول هذه الإشكالية بتطبيق **مُضاعف اسم الأسرة** على درجة القرب.

٥.٢ دلالة أسماء الأسر والقبائل

في مجتمعات الخليج، يحمل اسم الأسرة دلالات عن الانتماء القبلي والأصل الجغرافي والمكانة الاجتماعية. البحث باسم أسرة لا يعادل البحث عن اسم شائع في بيئة غربية — إنه أقرب إلى استقصاء مجتمع بأسره. استعلام واحد قد يُظهر بيانات عشرات أو مئات الأفراد دفعة واحدة.

٥.٣ معايير الخصوصية الثقافية والبيانات الجندرية

تختلف توقعات الخصوصية اختلافاً بنيوياً عن المعايير الغربية، خاصة في ما يتعلق بالبيانات الجندرية. قد يكون الحساب الرقمي عاماً تقنياً، لكن الأسرة والمجتمع يعاملانه بوصفه خاصاً فعلياً. يُطبّق البروتوكول **معدّلاً ثقافياً** يعكس هذه الفجوة.

٥.٤ إشكالية مجموعات المراسلة الجماعية

قد ينتمي الفرد إلى خمس عشرة إلى ثلاثين مجموعة نشطة، تضم كل واحدة عشرين إلى مئتي عضو. النفاذ إلى مجموعة واحدة يكشف أسرة كاملة أو شبكة مهنية بأسرها. يُلزم البروتوكول بتطبيق أقصى درجة قرب على جميع البيانات المستمدة من المجموعات.

٥.٥ ظاهرة العالم الصغير المهنية

في قطاعات التقنية والتقنية المالية والطاقة في الرياض وجدة، لا يفصل بين معظم المهنيين سوى درجة أو اثنتين. التحقيق في مسؤول تنفيذي واحد يكشف حتماً شريحة واسعة من منظومة القطاع.

٥.٦ بيانات الموقع في البيئات عالية الكثافة

كثافة النشاط في مدن الخليج تجعل كل نقطة موقع جغرافي ذات قيمة استدلالية عالية. يشترط البروتوكول إخفاء الطوابع الزمنية وتعميم الإحداثيات عند التخزين.

٥.٧ نظام حماية البيانات الشخصية

يُرسي النظام، النافذ منذ سبتمبر ٢٠٢٤، متطلبات مباشرة الصلة:

- **الموافقة الصريحة:** لا يجوز الجمع أو المعالجة دون موافقة صاحب البيانات.
- **تحديد الغرض:** لا يجوز إعادة توظيف البيانات لغرض مختلف.
- **مبدأ التقليل:** لا يُجمع إلا ما هو ضروري مباشرة.
- **ضوابط النقل العابر للحدود:** تتطلب ضمانات محددة.
- **العقوبات:** غرامات تصل إلى خمسة ملايين ريال والسجن المحتمل.

٥.٨ التحول الرقمي في إطار رؤية ٢٠٣٠

سرّعت المبادرة وتيرة الرقمنة بشكل غير مسبوق، مما أنشأ حجماً هائلاً من البيانات المتاحة. الفجوة بين وفرة البيانات ونضج آليات حمايتها تُوجد حاجة ملحّة لأطر عمل مثل ميزان.

٥.٩ توصيات التعديل

التعديل	التوصية
مضاعف القرب	تطبيق مُضاعف ١.٥ إلى ٢.٠ على درجات القرب.
معدّل الحساسية	إضافة ٠.٢ إلى ٠.٣ للبيانات الأسرية والجندرية.
تخفيض الاضطراب	خفض الحدّ المقبول بمقدار ٠.١ إلى ٠.٢.
عمليات الأسماء	إلزام مسوّغ أخلاقي صريح للبحث بأسماء الأسر.
بيانات المجموعات	تطبيق أقصى درجة قرب على بيانات المجموعات.

٦. بيان الحداثة والتفرد

لا يُقدّم أي إطار عمل قائم في هذا الحقل: معادلة رياضية لحساب المخاطر مسبقاً، ومنهجية تشغيلية معدومة التلامس مُدمجة مع الامتثال الأخلاقي، ومعيار توثيق لسلسلة العهدة يجمع بين الإثبات التقني والتبرير الأخلاقي — في بروتوكول واحد متكامل.

بروتوكول ميزان هو، حسب أفضل ما تُفيد به المراجعة المتاحة، أول إطار عمل يحقق هذا الدمج في بروتوكول واحد قابل للتكرار.

كلمة **ميزان** مشتقة من الجذر العربي «و ز ن» وتعني التوازن والمقياس. اختير الاسم لأن البروتوكول يعمل بوصفه ميزاناً يزن المخاطر الأخلاقية لكل خطوة قبل تنفيذها. يعكس الاسم الدقة الرياضية للإطار والسياق الحضاري الذي انبثق منه.

٧. القيمة العملية: لماذا يحتاج الممارس إلى ميزان؟

بروتوكول ميزان ليس تمريناً نظرياً ولا مساهمة أكاديمية مجردة. إنه أداة تشغيلية صُمّمت لحل مشكلات واقعية يواجهها ممارسو التحقيقات الرقمية يومياً. فيما يلي القيم الجوهرية التي يقدمها البروتوكول:

٧.١ الحماية القانونية للمحقق

مع تشديد أنظمة حماية البيانات عالمياً — من نظام حماية البيانات الشخصية في المملكة إلى اللائحة العامة لحماية البيانات في أوروبا — أصبح المحقق الرقمي معرّضاً لمسؤولية قانونية مباشرة. حين يُطعن في تحقيق أمام جهة قضائية أو تنظيمية، لا يكفي القول إن النية كانت حسنة. بروتوكول ميزان يوفر **سجلاً مُوثّقاً وقابلاً للمراجعة** يُثبت أن كل خطوة في التحقيق خضعت لتقييم أخلاقي مسبق ومُسوّغ رسمياً. هذا التوثيق يتحول إلى درع قانوني حقيقي.

٧.٢ توحيد المعايير بين الفرق

في المؤسسات التي تضم فريقاً من المحققين الرقميين — سواء في أمن المعلومات المؤسسي أو الصحافة الاستقصائية أو إنفاذ القانون — يعمل كل محقق حالياً بمعاييره الشخصية. النتيجة: تناقض في الأحكام الأخلاقية داخل الفريق الواحد. بروتوكول ميزان يُرسي **لغة قياسية مشتركة** للمخاطر الأخلاقية، مما يُمكّن من مراجعة النظراء والتصعيد المنهجي والتدريب الموحد.

٧.٣ بناء ثقة العميل والمُكلِّف

حين تُقدّم نتائج تحقيق لعميل أو جهة مُكلِّفة مع توقيعات إثبات السلوك الأخلاقي مرفقة بكل عنصر أدلة، فإنك تُوفّر مستوى شفافية يتجاوز ما يُقدّمه أي منافس. هذا يُميّز الممارس المحترف عن الهاوي، ويُحوّل الامتثال الأخلاقي من تكلفة إضافية إلى **ميزة تنافسية**.

٧.٤ الدمج مع أدوات التحقيق القائمة

صُمّم البروتوكول ليُدمج مع أدوات التحقيق القائمة لا ليستبدلها. حساب نصف قطر التأثير يمكن أتمتته بنصوص برمجية تتكامل مع أدوات الاستطلاع والتحليل المستخدمة فعلياً. إثبات السلوك الأخلاقي يمكن توليده آلياً عند كل عملية جمع. المنهجية ليست طبقة بيروقراطية تُبطئ العمل، بل **طبقة أمان** تحمي المحقق دون أن تُعيقه.

٧.٥ التدريب والتأهيل المهني

في غياب معايير موحدة، يصعب تدريب المحققين الجدد على الأخلاقيات بشكل منهجي. بروتوكول ميزان يوفر **إطاراً تعليمياً قابلاً للقياس**: يمكن تدريب المحقق على حساب درجة المخاطر، واختبار قدرته على تطبيق المنهجية في سيناريوهات واقعية، وتقييم أدائه بمعايير رقمية بدلاً من أحكام ذاتية. هذا يُسرّع بناء الكفاءات ويرفع مستوى الميدان بأسره.

٧.٦ سيناريوهات التطبيق الواقعي

السيناريو	القيمة المُقدَّمة
فريق أمن مؤسسي يحقق في تسريب بيانات	حساب المخاطر يمنع الفريق من تجاوز نطاق التحقيق وكشف بيانات موظفين غير معنيين. التوثيق يحمي المؤسسة قانونياً.

صحفي يحقق في شبكة فساد	المنهجية تضمن عدم كشف مصادر غير معنية. سلسلة العهدة تُعزّز مصداقية الأدلة عند النشر.
جهة إنفاذ قانون تبني ملفاً استخباراتياً	التوثيق يضمن قبول الأدلة أمام القضاء. حساب المخاطر يمنع الطعن في شرعية أساليب الجمع.
مستشار أمني يُقيّم بصمة رقمية لعميل	المنهجية تضمن عدم كشف العميل أثناء التقييم ذاته. التقارير المُوثّقة ترفع القيمة المهنية للخدمة.
باحث أكاديمي يدرس شبكات التضليل	الإطار يُلبّي متطلبات لجان أخلاقيات البحث العلمي ويوفر منهجية قابلة للتكرار والنشر.

٨. الخاتمة: نحو استخبارات رقمية دفاعية

بروتوكول ميزان ليس مجموعة توجيهات. إنه **بنية أمنية** صُمّمت للجيل القادم من المحققين الرقميين. من خلال إخضاع الأخلاقيات للقياس الكمّي، وفرض أساليب الحد الأدنى من التداخل، وتوثيق الامتثال بسلسلة عهدة رقمية أخلاقية — نُؤمّن حماية مزدوجة لموضوع التحقيق وللمحقق من المسؤوليات القانونية والأخلاقية والتشغيلية.

الطموح النهائي هو تحويل الاستخبارات مفتوحة المصدر من ممارسة اجتهادية عشوائية إلى علم هندسي منضبط — حيث يُعدّ الصمت الرقمي أرقى أشكال الإتقان المهني.