Crime, Law and Social Change (2025) 83:61
https://doi.org/10.1007/s10611-025-10248-z

Predictive policing in action: a field-based critique of the Italian case

Carlo Gatti[1]

Received: 27 June 2024 / Accepted: 17 November 2025

Abstract
In this article, I conduct an exploratory study based on first-hand information from developers and police agencies to outline the current implementation of predictive policing in Italy. While highlighting several actors' lack of responsiveness and transparency, the study elucidates a predictive tool's features and offers insights into the Italian context's peculiarities. Key aspects include the arguments for secrecy advocated by police agencies, the plans of the Department of Public Security for upcoming attempts to relaunch predictive policing, and the state of the predictive policing market, which, at the moment, appears dominated by buyers' scepticism and companies' struggle to still build their business image. Additionally, field-based reconstruction provides an overview of the main political and legal issues, which I deliberately broach from a non-privacy-centred perspective. Based on this analysis, I challenge the secrecy arguments and critique the dominant regulatory approach that focuses on 'profiling-like' outputs as the ultimate test for the lawfulness of AI-led predictions in law enforcement.

Keywords Predictive policing · Italy · Secrecy · AI Act

Introduction

'Predictive policing' (hereafter PP) refers to a set of practices based on algorithmic predictions to identify future police targets, either future offenders or future crime spots (Babuta & Oswald, 2019; Bachner, 2013; Ferguson, 2017a; Perry et al., 2013; Uchida, 2014). This distinction in targets translates into two types of possible algorithmic outputs, leading to the basic differentiation between person-based and place-based systems (Ferguson, 2017b).

✉ Carlo Gatti
carlo.c.gatti@utu.fi

[1] Faculty of Law, University of Turku, Turku, Finland

Published online: 01 December 2025

While some countries have been more extensively studied regarding the implementation of PP (Babuta & Oswald, 2019; Couchman, 2019; Gerstner, 2018; Oosterloo & Van Schie, 2018; Robinson & Koepke, 2016; Seidensticker et al., 2018), others have hitherto received less attention. Among these, Italy stands out as a country where the existence of PP technologies is confirmed by independent reports (Algorithm Watch, 2020; Fair Trials, 2021), scholarly papers (Gatti, 2022b; Grossi, 2020; Parodi & Sellaroli, 2019), and informative articles (Castigli, 2023; Morelli, 2019), as well as public statements by software providers.[1] Nonetheless, none of the Italy-focused studies engage in fieldwork in the strict sense, relying instead only on publicly available information. Italy-centred studies often highlight the difficulty of fathoming the algorithmic workings due to their proprietary nature but lack attempts to collect first-hand information. This gap precludes assessing the responsiveness and transparency of companies and police agencies or analysing the reasons adduced for any reluctance to talk. Moreover, Italy's EU membership calls for a more comprehensive analysis, especially with the recent introduction of the AI Act, while other EU provisions (Directive EU 2016/680) have so far addressed automation in law enforcement with limited success.

Thus, the main gap this paper intends to fill is advancing knowledge of PP in Italy by overcoming the barrier of publicly available sources. Notably, this study does not aim to be comparative. This decision reflects a clear methodological stance, grounded in both epistemological and practical considerations. The study is designed as a field-based inquiry into a national context that remains empirically understudied. Epistemologically, the aim is to produce context-sensitive knowledge by linking empirical findings to the legal and institutional framework in which PP technologies are deployed. While references to other countries are occasionally used, they serve only to provide context by highlighting peculiarities of the Italian case, frame subtopics of PP studies, or to contrast the Italian scenario with broader trends. These references, drawn from publicly available studies and reports, are instrumental to the main Italy-centred analytical thread, which is based on first-hand sources. This approach is also grounded in feasibility: conducting multi-country fieldwork would have required a different research infrastructure and would have compromised the granularity of the Italian case reconstruction.

With this in mind, the paper addresses three interlinked RQs:—*What is the overall level of responsiveness and transparency of private developers and police agencies using predictive PP algorithms in Italy*?—*What new knowledge, compared to public information, is attainable about the functioning and the use of these systems*?—*What legal and political issues emerge from the field research?*

In pursuit of first-hand insights, the study engages private developers and institutional users of two proprietary predictive systems (herein referred to as 'Software A' and 'Software B'), reported in the literature as the representatives of PP in Italy. Analysing companies' and users' responsiveness is crucial for the ongoing debate on the expansion of predictive technologies and for tracking major legal and political implications based on field evidence. At the same time, my aim is not to map every

[1] Full references to authors and websites are intentionally avoided to avoid disclosing the companies' identities. The reasons for non-disclosure are explained in the methodological section.

aspect susceptible to legal assessment, but to unearth legal questions often overshadowed by a privacy-centred approach (Levano, 2024; Lynskey, 2019). While privacy is undoubtedly key in other legal branches, its centrality appears questionable in law enforcement, as the possible overrun of privacy is precisely one of the defining raison d'être of police function (Millett et al., 2007). This is not to imply that everything done in the name of crime prevention is lawful, but rather that the lawfulness should be primarily assessed—and questioned— on grounds other than privacy rights.

Although not delving into deep theoretical discussions, the underlying background is radical criminology (Hulsman, 1986; Platt, 1974), particularly the intersection between materialist approaches to criminal selectivity (Gatti, 2023; Baratta, 1989; Taylor et al., 1973) and police power (Neocleous, 2021). In terms of structure, the paper unfolds as follows: I first illustrate the methodological steps; next, I present the data collected during the fieldwork, organising them into subsections reflecting three groups of respondents (Software A, Software B, and addressees unrelated to the design or use of any software); I then provide, in the discussion, an overview of the most significant findings that emerged from the fieldwork, broken down into subsections; finally, I conclude by appraising the main takeaways and envisaging avenues for future research.

Methods

This study, conducted through 2023 and 2024, aimed to collect first-hand data from vendors and users of two predictive tools identified in literature as the only examples of PP in Italy. Given the challenges in similar studies (Algorithm Watch, 2020; Couchman, 2019; Fair Trials, 2021; Grossi, 2020; Neslen, 2021)—with exceptions to secretiveness only with non-proprietary systems (Oosterloo & Van Schie, 2018)—preliminary crosschecks were advisable before contacting companies and police HQs.

I initiated a round of informal exchanges and calls with professionals who, due to their experience and position, might possess knowledge beyond publicly available information and have a genuine interest in the research results. This initial step served as a trial phase to assess my initial knowledge and recalibrate the fieldwork strategy. The conversations involved Fabio Chiusi, a research associate and project manager in 'Automation on the Move' at AlgorithmWatch; the Italian law firm 'Martorana', specialising in Law & AI and gaining mounting authority nationwide; and two Italy-based civil liberties groups for digital rights belonging to the European network 'EDRI': Hermes Center for Digital Rights and CILD (Civil Liberties in the Digital Age). These conversations confirmed the necessity of engaging directly with software designers and users, as no additional knowledge beyond publicly available information was found.

Aware of possible adversarial attitudes, respondents from vendors and police forces were not sampled at source, as any reduction in their number could further minimise the chances of fruitful contacts and preclude representations of overall responsiveness. The fieldwork proceeded by first locating the companies developing

the algorithms cited in the literature (hereafter 'Company A' and 'Company B') and all the police HQs using one or the other system. While the list of 'Software B' users was easily traceable on the company website (more details below), the list of 'Software A' users was initially unclear. In terms of trade history, both tools were first beta-tested by a few police departments until approximately 2020–2021, before being brought to market in their current trademarked form. This circumstance accounts for the internal differentiation, particularly relevant to 'Software B', between beta-testers and current users.

Companies and police HQs were sent written requests containing an invitation to a semi-structured interview (Bradford & Cullen, 2012), with content slightly varying according to the respondent category. In the emails to companies, the interviews were announced to address: 1) technical characteristics of the software (type of target crimes, type of output, source of input data, predictive markers); 2) implementation stage and areas where the system is in use; 3) possible legal obstacles encountered during development or implementation. Regarding inquiries to the police HQs, the interview topics covered: 1) the technical characteristics of the software, and 2) the officer's role and perception of the procedure (procedure comprehensibility and additional help beyond previous contextual knowledge). Reflecting on the contact-making context, the interview format could be considered semi-structured due to the open nature of questions allowing for explorations not estimable a priori, yet not implying any laborious self-reflective meaning construction or participants' conceptualisations, typically associated with the term 'semi-structured'.

Thus, in stating the overall research purpose (Galletta & Cross, 2013), I specified in my emails that no interview would be recorded (only transcribed) and the names of the respondents, companies, and police departments would remain confidential. These measures sought to build trust by averting both reticence deriving from the disclosure of personal, institutional or business identity and by mitigating feelings of power imbalance induced by the recording device, although, as Alvesalo-Kuusi and Whyte (2018) emphasise, when 'studying up' powerful, questions of power should always be situated within broader social power imbalances, beyond the immediate research relationship.

Besides conveying the interview proposal, the written requests served as gauges for responsiveness and potential triggers to multi-round written exchanges. Thus, answers by public authorities such as arguments for secrecy, or claims by police HQs to have only beta-tested a software no longer in use—allegedly making it impossible to find personnel for interviews – invariably prompted follow-up questions: for instance, as to why the algorithm had been discontinued. It is worth noting that only in one case was the final interview granted (Company A), while all other interactions occurred via written exchanges.

The challenge of securing interviews, emerging since the first attempts, resulted in a greater reliance on written exchanges, confirming the appropriateness of avoiding sampling. All participants engaging in written exchanges provided consent for their answers to be included in the research data.

All recipient inboxes consisted of corporate or institutional emails retrieved from the websites of the companies, the municipal governments, or the Ministry of Interior. Given the relevance of each communication step, recipients were categorised as

'non-respondents' only after four unsuccessful contact attempts, with the third one being a "reinforced" contact modality. For small-size HQs, this entailed phone calls to inquire directly about relevant information and/or to obtain internal contacts—not available online—to which the original request could be re-forwarded immediately after the call. As for larger municipalities, if a third attempt proved necessary, this consisted of copying the original message to at least one department head and the municipal councillor for transparency, since in medium-to-large municipalities these contacts are retrievable from institutional websites, whereas the phone numbers available online are often general and external call centres. If needed, a fourth attempt involved sending legally certified emails (PEC) from a fee-paying mailbox specifically activated to the same addressees used in the third round, so that no respondent could claim delivery failures. Only when not reacting to this fourth attempt were surveyed labelled as "non-respondents". Additionally, although not initially part of the research design, the Italian Data Protection Authority (GPDP) and the Department of Public Security (DPS) were also surveyed.

Data and results

Software A

From public information, we know that 'Software A' is a predictive tool focussing on commercial robberies in the urban space. Due to both scant literature on its operating principles and the unclear identification of its actual users, data collection could only begin by contacting the manufacturer ('Company A'). These contacts led to an interview with a company executive, in which the respondent illustrated the algorithm's features by first introducing two operating guidelines. First, the algorithm resorts to machine learning, but not to any deep-learning or neural network system. Second, the predictive projection must be explained as a co-result of automated 'crime linking', namely, the detection of past criminal incidents belonging to the same criminal series (i.e., to the same perpetrator). According to the 'Company A' representative, "*the starting problem* (from the police viewpoint) *was to solve past cases and the need to uniform the data collection procedure. Automated crime linking is enabled precisely by detecting little pieces of behavioural information that usually go unnoticed under traditional policing".* Thus, the prediction of the time/place of the next criminal episode—hence the apprehension of the perpetrator before the offence is committed – follows the linkage of different criminal occurrences, apparently unconnected, within the same sequence: the recurring hallmarks on which the clustering builds will also enable the prediction of the next occurrence. By positing that *"everything is behavioural"* and *"we are repetitive in our behaviours",* the respondent argued that *"the usual balance between conscious and unconscious behaviours is altered under the stress typical of committing a crime. Under this pressure, the unconscious ethological components tend to become dominant and reveal the perpetrator's 'behavioural footprint'*". The intrinsic limitation of this approach is that it only applies to offences assumed to be serial.

When asked for the markers, the interviewee clarified that a full list could not be provided because of both the trademark policy and the practical complexity of such an enumeration. However, the respondent described the markers as consisting of unconscious ethological components summarised in four categories: "*proxemics, kinesics, verbal and paraverbal components"*; complemented by general information about the crime target (type of commercial establishment and time/location). To the specific question regarding the use of socioeconomic or demographic data of the areas, the respondent answered that at no time these were factored in, as "*in the system only police data are used, that is, data collected by police officers in the immediacy of the incident through direct surveys, victim's testimony, security footage"*. This is congruent with markers focussing on behavioural aspects and the crime spot description.

The output consists of a spatiotemporal prediction about the next crime spot, combined with an abstract identikit based precisely on those behavioural hallmarks underpinning the linkage. Importantly, when the predictive output is delivered, the identity is still unknown *("otherwise the offender(s) would have been already arrested"),* while the identikit only comprises ethological and physical features recurring throughout the (supposedly) same series, which should guide the police to the next crime spot. Unlike the risk assessment typical of person-based PP, the 'identikit' here has nothing to do with assessing targeted natural persons by predefined risk factors, as the variables enabling crime-linking are not risk factors per se. They are 'predictive' because, in retrospectively linking different events, they enable 'unveiling' a single chain and thus the place of the next occurrence. The respondent confirmed that linking variables are never automatically exported to future iterations, as, unlike the actuarial approach (Harcourt, 2003), their relevance is purely internal to the single crime-linking operation. When questioned about the user's role, the 'Company A' representative claimed that *"the analytical part of the algorithm is visible and police forces get access to the elements determining the crime linking hypothesis. This is proposed to the user according to two different degrees of probability ('simple hypothesis' or 'highly likely hypothesis') and always needs to be user-validated.*

On the sidelines of technical descriptions, the interviewee made two additional remarks on the validity of the software. The first suggests an internal clash between different approaches to PP, with harsh criticism of the dominant PP mode from the same business sector. In the respondent's words *"Only the arrest* (i.e., the arrest enabled by predictive crime-linking) *stops the criminal series, whereas hotspot policing does nothing but move crime elsewhere"*. The second observation, quite unusual among PP promoters, is the praise of the software's performance in terms of "*labour-savingness for prosecutors looking for evidentiary material".* Indeed, the idea behind 'Software A' is to apprehend someone just about to commit the predicted crime, while punishing them for past offences within the series. This is why, the interviewee says, *"Sometimes, the defendants themselves confessed to further episodes of the same criminal series, especially when confession did not impact the length of their sentence. This allowed a gradual cleansing and coordination between fragments of information previously unknown or left in isolation".*

Regarding 'Software A' users, the respondent reported that the system is currently used only in the original beta-tester police department (provided with the beta-ver-

sion on free loan), also specifying that the company *"is still not making money from the software"*. The scenario depicted by 'Company A' is one where the trademarked software has not found any buyers yet, while the only on-field application concerns the beta version given to the original tester (hereafter 'HQ A', being the only police HQ related to 'Software A'). Upon probing 'HQ A' following this information, they responded that the headquarters has not used the software since 2021 and, due to subsequent personnel turnover, no officer would be able to give interviews from the user's perspective. The discrepancy with 'Company A' answer is undeniable, but it does not necessarily reveal bad faith. The precinct has presumably stopped using the beta version without informing the company, especially considering the free loan scheme. The fact remains—just as stated by 'Company A' – that they have not made any business profit so far. The point is rather why the beta-tester abandoned the tool at some point, but when surveyed on this, 'HQ A' did not answer, which led me to reiterate the same question to the DPS (see below).

Software B

The main premise regarding 'Software B' is the vendor's lack of responsiveness. Four contact attempts over ten months were made with 'Company B' unfruitfully, using both general corporate contacts and a mailbox specifically created for software purchasers. Considering the timeframe and the high business interest behind the product-dedicated mailbox, missed reading is implausible. However, from publicly available information, we know that 'Software B' is a typical predictive hotspot tool for predatory crimes in the urban environment (mugging, robberies, petty thefts, and shoplifting) that builds on criminological theories such as routine activity, situational crime prevention and broken windows. The interface is a heatmap where varying risks of future crimes are associated with different spots, with the output consisting of a georeferenced alert. According to 'Company B' website, the algorithm was first beta-tested by six police HQs (testers 1–6) until 2021 and is currently employed in its trademarked version in 21 municipalities (users 1–21). However, this apparent expansive trend vanishes upon closer examination. *First*, none of the institutional beta testers are current users. In other words, none of the testers decided to keep it. *Second*, while the testing phase was conducted by National Police HQs ('Questure') of six medium-to-large towns, the current 21 declared users are Local Police Departments, meaning they depend on the Municipality, not the Ministry of Interior. *Third*, whilst the six beta-testers were all provincial capitals (two of which are regional capitals), the 21 current users comprise 15 non-provincial municipalities and only six provincial capitals, none of which are regional capitals. When quantifying these variations, the result is remarkable. Whether we observe the 'test-current use' transition by population or area under jurisdiction, we witness a reduction of approx. 80% and 90%, respectively, with even greater variations when referring to average values (see Table 3).

Thus, despite the company's inertia, publicly available data were sufficient to list and contact the Police HQs using Software B. Among the six beta testers, testers 3 and 6 did not respond, while Testers 1, 2, 4, and 5 proved reactive, although no interview could be arranged following the initial survey. The reason given by all four

responding HQs was the difficulty of finding suitable interviewees because of the lapse since they stopped using the algorithm (approx. three years). The interchange with the responding HQs continued to explore more about the technical characteristics of the software and the reasons for stopping its use at a given moment. At this point, tester 4 stopped engaging in further exchange. Testers 1 and 5 denied explanations about the decision to quit the algorithm, but both justified the nondisclosure of the inner workings by claiming that "*it is not possible to provide the requested insights, given the cruciality, at the departmental level of the Ministry of the Interior* (i.e. the DPS)*, of the design of the aforementioned software or any other predictive crime analysis systems*" (Tester 1), and that *"the instrumental reasons behind the termination of the use of 'Software B' cannot be disclosed"* (Tester 5). As for tester 2, conversations were held with the current police chief, who joined the HQ in December 2023. In his words: *"based on the information I have, this Police HQ beta-tested 'Software B' but stopped using it in 2020. I do not know the specific reasons behind this interruption, and the chief in charge at that time is now retired. However, I am afraid that even if I knew them, the DPS should be consulted before delivering any answer".* This last caveat, combined with the inputs from testers 1 and 5, prompted me to address directly the DPS.

As regards the current users listed on Company B's website, 12 Local Police HQs out of 21 were catalogued as 'non-respondents' after unfruitfully exhausting the contact attempts described in the methodological section.

Seven other HQs (Users 7, 12, 14, 15, 16, 17, 19) did not grant interviews on the algorithm for the quite surprising reason that, in the words of their representatives, the software has never been used in their precincts. Many of them also stressed never having heard of the company name. User 17 nearly reached self-irony when explaining that "*we are the Local Police: we just intervene on what happens around when we are out on duty*. *Sometimes, we cannot even act on what happens, let alone predict what will happen*".

Confirmations about the current use of the software came instead from Users 6 and 20. Nevertheless, not even these Police Departments agreed to be interviewed according to the initial request. User 6 explained that "*Software B has recently been integrated into our operations centre. It is currently being tested* (ed.: not in the sense of beta-tested) *and we have no operators who are using it regularly. Consequently, we are currently in no position to give you an evaluation or an impression of its usefulness and thus fulfil your request. However, I invite you to contact us again in about a year*". The subsequent proposal for a shorter interview concerning only the operational characteristics of the algorithm—excluding officers' perceptions or evaluations—remained unanswered. This made it impossible to determine whether the rejection of even a shorter interview was due to 'corporatist' claims of public security or the vendor's business policy. User 20, in turn, added an important piece, which led to the involvement of the GPDP (see next subsection). Their motivation for not providing detailed information was that: "*the software was used by us for a very short period only, as almost immediately the Italian Data Protection Authority—Department of Legal Affairs and Justice—opened a proceeding aimed at verifying the correct data processing. This led the Municipal Administration to suspend, as a precautionary measure, the use of 'Software B'".* They confirmed that "*no reinstate-*

ment is scheduled at present", claiming no knowledge of other municipalities in a similar situation.

Italian data protection authority and department of public security

As a result of the exchange with User 20, a formal request was sent to the GPDP demanding further explanations on three basic points: 1- when the proceedings were initiated so that User 20's precautionary suspension could be chronologically placed; 2- whether similar proceedings concerned other municipalities using the same software; 3- whether the proceeding aimed at attaining the list of predictive variables and, if so, whether the list could be disclosed to the public once the proceeding was over. After the request's filing and some weeks of waiting, the GPDP's Department of Justice and Security Affairs replied: "*In the second half of 2021, this Department opened a preliminary investigation aimed at acquiring information on a PP project attributable to 'User 20'. Based on the information received from the municipality, it emerged that the project did not comply with current legislation on personal data protection, and this was communicated to the Municipality. This appears consistent with what the Local Police told you regarding the suspension of the project following the initiatives taken by this Authority. After that, no further communications were received from the Municipality on that project, so the file was archived.*" The answer, complemented by the caveat that no further information was disclosable, was far from exhaustive. I then resumed the exchange to at least clarify some statements contained in their reply, in particular:—whether the non-disclosure of the criticalities and operational characteristics of the system is due to the proprietary nature of the software or to a different legal basis;—whether the wording "initiatives taken by this Authority" hints at *ex-officio* initiation or instead a third-party complaint was the trigger. Unfortunately, neither new answers nor notifications of filing (as occurred with the original petition) followed my request.

In parallel, following the conversations held with 'HQ A' and 'Software B' testers, I addressed the DPS to clarify whether a common reason existed for the beta testers of both systems having quit them, especially given their evasiveness or declared intention not to provide explanations bypassing the DPS filter. Upon being asked directly, the DPS stated that: "'Software A'*, used exclusively by* 'HQ A'*, and* 'Software B*', initially used by* 'Testers 1–6*'were developed and tested free of charge as tools for analysis and georeferencing of crime. From 2021, the operation of the aforementioned applications in the Police offices has been suspended, as it was deemed preferable to develop a proprietary software called 'GIOVE'. This system, which is still being developed, will make it possible to increase the response capacity to crime, both preventive and repressive, through the processing of information that will also support judicial decision-making thanks to the identification of common circumstances relating to apparently different facts. The GIOVE software is currently being evaluated by the Authority for the Protection of Personal Data* (GPDP)". When asked about what company would be behind this new proprietary software and whether this system drew inspiration from 'Software A' given the clear operational similarity emerging from their description, the DPS pointed out that their first answer should be understood as "*exhaustive of the amount of information disclosable at the moment*".

Discussion

Responsiveness

Addressing the issue of 'responsiveness' as a prerequisite for data access, the research reveals a concerning lack thereof. This is particularly significant given the frequent calls for transparent and explainable AI in sensitive areas where public authorities should readily seize any opportunity to clarify their work procedures. In general, unresponsiveness was observed among both police agencies and companies, albeit in different terms. Companies exhibited the extremities of the spectrum of reactions: whilst 'Company A' demonstrated good openness and was the only respondent to grant an interview, 'Company B' did not even provide any written reply. As for the Police HQs, half of them (14 out of 28 including testers and users) remained completely unresponsive. Among those actively responding, five HQs expressed the position proper of the testers; seven HQs opened up the unexpected scenario of denying any use of the algorithm or even knowledge of the vendor's name; two confirmed having used the algorithm (User 6, User 20). It is important to note that responsiveness serves as a preliminary criterion for distinguishing responding participants from non-respondents. The assessment of the answers' actual contribution to the research is addressed in the subsequent subsections.

Data accessibility: secrecy claims

In the context of PP studies, arguments for secrecy are often presented in two main forms: trade secrecy and the anti-circumvention argument. Trade secrecy, which protects proprietary information from a business-oriented perspective, is widely recognised by scholars as a typical obstacle to algorithm accessibility (Joh, 2017; Moore, 2017). The European Crime Prevention Network also highlights the need for transparency, suggesting that "to further facilitate transparency, it is imperative to rely on in-house software developers rather than commercial companies" (EUCPN, 2022:14). In contrast, the anti-circumvention argument (Bloch-Wehba, 2021; Manes, 2020) posits that knowledge of surveillance technologies could enable individuals to evade supervision.

Common to both companies was the non-disclosure of full lists of predictive markers. Nevertheless, a 'Company A' representative described the typology of markers, significantly advancing the understanding of 'Software A' and allowing for both legal and political assessments.

Regarding information openness demonstrated by Police HQs, their answers, even when providing pieces of information, were primarily arguments to evade final interviews. Beta testers' explanations, appealing to the elapsed years since the testing's termination, appeared at least sounder than answers by current users. Testers 1, 2, and 5 were also more explicit in advocating for non-disclosure of the algorithms' operating features.

Interestingly, Italian police appeal not to commercial secrecy but to the role of these technologies in crime prevention, in line with the DPS. Since my research aimed to unveil general presumptive criteria rather than data about individuals or

ongoing investigations, the integrity of criminal proceedings cannot be at stake.[2]It follows that their non-disclosure claim exemplifies an 'anti-circumvention' argument (Manes, 2020). However, we do know that predictive variables used by traditional place-based systems generally incorporate static demographic descriptors such as historical crime data, well-being indicators, or infrastructure location data (Europol, 2024; Lorenz et al., 2021, Lum & Isaac, 2016; Oosterloo & Van Schie, 2018; Robinson & Koepke, 2016; Seidenstcker et al., 2018). This study, in addition, reveals the use of "unconscious behavioural components" by 'Software A'. Therefore, predictive variables mostly appear as markers not alterable at the subject's will, either because they are static or encapsulate unconscious elements. These circumstances render the risk of opportunistic strategies to evade supervision unlikely and the anti-circumvention rationale groundless. Moreover, 'anti-circumvention' alone does not justify secrecy in any crime prevention activity. Otherwise, it should also remain secret under which circumstances the police can use wiretaps (Manes, 2020).

Regardless of the markers' nature, the roots of secrecy should be preliminarily questioned by the 'principle of legality' in criminal law, enshrined in the formula *nullum crimen, nulla poena sine lege* (Hallevy, 2010; Weyembergh & Galli, 2013). This principle requires that any offence and corresponding penalty be defined in a statutory act accessible to anyone subject to it. Interpreting algorithmic variables as new or atypical legal sources would be a strained reading. However, the principle of legality extends beyond the procedural duty for legislators to define offences and penalties in statutory provisions and citizens' right to access these sources. Historically, it reflects a deeper expectation for citizens to estimate at any time the institutional reaction against legally qualified situations. Secrecy over codes and markers that 'formalise'—as they automate—presumptive criteria directly conflicts with this precept.

Therefore, the principle of legality, rather than privacy, should be the primary lever to override non-disclosure claims, whether justified by trade secrecy or 'anti-circumvention' arguments. Additionally, the trial-oriented nature of 'Software A' amplifies secrecy-related conflicts, as its predictions serve as evidentiary elements linking past events and determining longer sentences. Maintaining secrecy about the presumptive criteria for crime-series construction raises issues concerning open proceedings and potential conflicts with Article 6 ECHR. Although the lack of current 'Software A' users makes this threat not imminent, similar procedural issues may arise in the future with GIOVE, given its 'Software A'-like functioning announced by the DPS.

Finally, the right to explanation under AI Act Art. 86 cannot resolve secrecy issues, given the exceptions in its paragraph 2, including those in EU Directive 2016/680 Art. 13(3), which grant States broad discretion in restricting or omitting information provision in law enforcement.

[2] In other words, 'sensitive operational data' as defined in AI Act art. 3(38) are not at stake here. The AI Act seems clear in treating 'sensitive operational data' as ex-post information emerging from completed iterations about specific individuals, something different from knowing *in abstracto* the type of input data. Consistently, the disclosure of 'sensitive operational data' is regulated as potentially problematic only in the context of developers-deployers relationships in the post-market monitoring, and between the deployers and the market surveillance authorities (art. 5 AI Act).

Data accessibility: end of testing and current use

Turning to why none of the beta-testers retained the algorithms post-testing, only the DPS provided a response that was not purely evasive. However, while the beta-testers also confirmed the termination of the testing around 2021, DPS' attribution of this to the development of the new system 'GIOVE' lacks credibility due to the time lag (as of January 2025, 'GIOVE' is still under development) and other events that emerged from the research. These include the trademarking of both systems and the confirmed use of the trademarked 'Software B' in at least two Police HQs (Users 6 and 20) during the research period. Interestingly, User 6, explaining the current impossibility of giving interviews, invited me to talk again in one year, assuming the system's uptime would continue. By withholding these circumstances, the DPS avoided mentioning the GPDP investigation "leaked" by User 20.

Regarding reactions from 'current users', it is notable that this group is limited to 'Software B'. Several Police HQs denied ever using the software, contradicting the company's webpage. Establishing whether these are cases of non-use after purchase or false claims by the company to enhance credibility might be challenging. However, the latter hypothesis seems the only plausible for several reasons. First, the Police HQs exposed themselves through written or oral exchanges, while the company remained unresponsive. Second, the Police HQs' answers often included elements of peremptoriness: in three cases (Users 12, 15, 17), the officers had never heard of the company, while in two cases (Users 7, 14), local police chiefs personally denied any use of the software, having no reason to expose the administration to justify the purchase of an unused tool. Less compromising answers could have justified non-use as accidental or temporary. Third, all such answers came from small villages, none of which are provincial capitals, suggesting that false claims could have been selectively applied to less known centres to expand the user list with minimal risk of denial.

Among the Police HQs confirming the uptime of 'Software B', User 6 stressed its occasional use, hence the lack of field-trained officers for interviews. While inviting me to contact them again in one year, my subsequent proposal for a technical interview went unanswered. This, along with the initial reply, suggests a perceived ineffectiveness of the tool. In turn, User 20, while not providing field use information, revealed the existence of a GPDP investigation, which might further explain the unresponsiveness of both ‘Company B’ and other Police HQs.

Predictive markers

Any consideration about the lawfulness of the predictive markers must reckon with the inaccessibility of detailed input lists. Without re-entering the soundness of non-disclosure claims, it is necessary to clarify that both systems, in principle, would be compatible with the AI Act. The list of AI practices prohibited by art. 5(d) includes only the use of AI systems for making risk assessments of natural persons, based “solely” on their profiling or on assessing their personality traits. This narrow delimitation permits any AI systems whose outputs do not involve profiling natural persons, including both traditional place-based tools like software B and systems like software

A, where behavioural characteristics are not the subject of risk assessment. The classification of software A and software B as high-risk under Article 6 Annex III is also not straightforward, and, even in that case, both could operate under the AI Act, subject only to more stringent post-sale monitoring.

Having cleared this initial legal hurdle regarding the system type, the types of markers revealed by the interviewee from 'Company A' (proxemics, kinesics, verbal and paraverbal components) do not seem to raise issues either in strictly legal terms: besides consisting of police data traditionally collected at crime scenes, in the fabric of 'Software A' they act not as risk factors, but as connectors for crime linking. Neither different data sources nor socio-demographic variables are involved. There are, however, some political issues emerging from the implicit endorsement of selective incapacitation theory (Greenwood & Abrahamse, 1982). This posits that a small group of offenders account for a large percentage of crimes, implying that crime could be nearly neutralised by identifying and selectively imprisoning them based on their dangerousness. The algorithm's focus on crime series, intended to provide prosecutors with the foundation for longer convictions, reveals how the main purpose is not so much prediction itself, but rather issuing longer prison sentences as the solution to crime ("*only the arrest stops the series*").

However, emphasising the importance of connecting repetitive events carries significant political implications. The concept of 'repetitiveness' in something as heterogeneous as crime implicitly validates the law-enforcement practices that have historically shaped this 'quality' as intrinsic to certain offences. Statistical frequency often results from reporting habits influenced by cultural factors or systematic overpolicing of specific sectors. Other crimes may appear less frequent simply because they escape general public awareness (e.g., corporate crimes) or require legally qualified perpetrators (e.g., corruption, abuse of office). Repetitiveness is also tied to the traceability of crimes within urban spaces. The spatiotemporal context of repetitive offences reflects a view of crime as a routine activity deliberately replacing legal livelihoods, confined to those 'needing' to commit crime. Assuming an underlying 'necessity' is the tacit precondition for predictable patterns, while crimes occurring in non-urban, virtual, or non-immediately perceivable environments—typically associated with the upper classes—remain outside the 'repetitiveness radar'.

Turning to 'Software B', while recalling the admissibility of this type of system under the AI Act, a thorough legal assessment of the markers cannot be made without detailed information from the company about the input data. Nonetheless, public sources, including a book by the software creator, indicate that the software is a typical place-based system that delivers risk assessments on potential future spots of urban predatory crimes. The underpinning theories are said to be Routine Activity, Situational Crime Prevention, and Broken Windows. The same book states that the predictive calculation follows a structural parallelism between crime and job performance under a wage regime, suggesting that lawbreakers need to offend a certain number of times a month to meet life necessities, much like regular workers seek monthly earnings. Like in a regular pay cycle, offenders aim to achieve their goals by a pre-established date. With this 'crime phenomenology' in the backdrop, it is likely that what Oosterloo and Van Schie (2018) found in the Netherlands may recur here. Their study demonstrates how a purely place-based output may involve extensive

mining of residents' personal and demographic information at the input level, which constitute the true 'ingredients' of the geo-referenced prediction.[3]Contrary to the presumption that the input data processed by place-based systems are limited to 'crime type', 'crime location', and 'timing data' (Lynskey, 2019), the risk assessment may easily transcend the smokescreen of the mapping infrastructure, including proxies for sensitive data as the real predictors. This is especially relevant considering that the investigation opened by GPDP against User 20, which led to the precautionary suspension of the tool, was based on data protection legislation infringements. Moreover, one should not underestimate the circumstance of the DPS's decision to launch, under the aegis of public authority, a new system mimicking Software A, rather than usual predictive mapping.

In sum, while a conclusive and detailed legal assessment of 'Software B' markers is not possible, a broader picture can be assembled from public information about the ideas inspiring 'Software B', the company's persistent unresponsiveness, the opening of a GPDP investigation for data protection violations, the system's suspension without a reinstatement date in the municipality under investigation, and the interchangeability at the input level between place-based and person-based predictors confirmed by previous studies. As a result, two interconnected issues raise a high alert: serious doubts about the lawfulness of the input data in use (unlike 'Software A'); and, like 'Software A', the implementation of an incapacitation-oriented agenda, which is difficult to reconcile with Italian constitutional mandates.

Beyond stated words: a business battle behind users' scepticism?

Parallel to analysing the answers and the gaps left unfilled in the exchanges with respondents, a meta-reflection on the big picture reveals dimensions crosscutting the phenomenon as a whole. A key issue that emerges is a generalised mistrust in the effectiveness of PP. Regardless of the explanation in each case, it is a fact that none of the beta testers of either algorithm decided to continue using the software. Conversely, none of the current (or presumed) users participated in the beta-testing. Currently, no police department is using Software A, while only two police HQs confirmed having used Software B at some point. One of these (User 6) does not use it regularly, while the other (User 20) suspended its operation following a GPDP investigation.

Even assuming the number of current users stated on 'Company B's website, the trend in software usage would not indicate growth, as the 'expansion' from six testers to 21 users, upon closer examination, corresponds to an 80 to 90% reduction in both

[3] Less striking but still significant examples of systems delivering location-based outputs while factoring in data such as population age, gender, nationality, household income, household composition, and education level are the place-based tools 'PAVED' in France and, to a lesser extent, 'Krimpro' in Berlin (Lorenz et al., 2021). This trend appears to be confirmed also in Spain, where a recent report documents the use of sensitive personal data—including health and social status—as predictive markers in a place-based system (Algorace, 2025, p. 21). On a theoretical level, the person/place dichotomy has been critically addressed within the critique of crime prediction rationalisations (Gatti, 2022a; Harcourt, 2007), and has also been problematised in other disciplinary fields, including media studies and urban geography (Pavoni & Tulumello, 2023).

territory and citizenry potentially affected (see Table 3). Moreover, Company B's attempt to corroborate an expansive projection is refuted not only by these statistics but also by several police precincts contradicting their status as users. This directly connects to a generalised scepticism surrounding a business sector still underdeveloped compared to other countries. Framing these dynamics as potential epiphenomena of a business battle can also explain the unusual tendency of 'Company B' to exaggerate the extent of predictive technology use. This is unusual because, typically, once established as a business sector, the trend is rather to withhold information on the real scale of technology use to avoid public scrutiny (Bloch-Wehba, 2021).

An unestablished market, with unclear hegemonic positions, likely drives high internal competition. This is exemplified by the heated debate highlighted by the 'Company A' executive between the crime-linking model of 'Software A' and the predictive crime mapping used by 'Software B', which was portrayed as pointless. GIOVE, the new predictive system currently being developed under the aegis of the DPS, represents the next frontier in this business battle, which is also a contest between predictive models. Correspondence with the DPS indicates that the software will be proprietary and its technology similar to that of 'Software A', which is also the predictive model with fewer risks of rights infringement regarding the input data (see previous subsection). While we cannot definitively assert that this was the reason for choosing a 'Software A'-like technology, PP strategies in Italy will enter a new phase, with one private company promoted to DPS partner. This also means that, contrary to EUCPN (2022) recommendations, the Italian strategy remains anchored to a proprietary scheme, while the DPS plays a role questionably integral to the public–private commingling by labelling the information about the company involved in GIOVE's design as "non-disclosable".

Concluding thoughts

The purpose of this paper was to provide a fieldwork-based account of the current implementation of PP in Italy, primarily drawing on first-hand information. Answering the first RQ, a constant theme throughout the study is significant resistance to responsiveness and transparency, which inevitably affected areas covered by subsequent RQs. Regarding the two vendors, the problem particularly concerns 'Company B'. As for police agencies, these exhibit a generalised inability to perceive themselves as having a duty to respond based on their institutional functions. Even when responses were granted, they mostly provided arguments to evade further questioning, confirming the persistence of a transparency problem. A surprising exception was 'Company A', which stood out as the most reactive of all respondents.

Despite these limitations, and to answer the second RQ, new knowledge compared to previous public information was acquired in three areas. *First*, through the interview with a representative from 'Company A', new insights were gained into 'Software A' technology. Notably, the study discovered that the system is not currently used by any Police HQ. *Second*, although new details about the inner workings of 'Software B' were not disclosed due to the company's unresponsiveness, several elements allowed for deconstructing the expansive image from beta testing to current

usage. The reality is a market far from consolidated, with companies striving to build corporate credibility. The failure of PP as a market sector seems confirmed—besides the non-use of 'Software A'—by a simple comparison of demographic and territorial statistics between testing areas and territories where 'Software B' is currently declared in use by the company. Further investigation reveals that several Police HQs listed as current users are not such when questioned. *Third*, the involvement of responders not initially included in the research design brought to light two previously unknown circumstances: the development of new proprietary software with the blessing of the DPS and an investigation opened against one 'Software B' user by the GPDP.

Moving to the third RQ, the first legal and political issue concerns how the non-disclosure of the algorithms' inner workings is justified. While 'Company A' invokes trade secrecy solely to withhold a detailed list of markers, the explanations provided regarding the types of predictive variables enable a reasonable understanding of the algorithm's mechanics. In contrast, Italian police adopt the 'anti-circumvention argument', exhibiting a hermeticity that permeates police bodies irrespective of vendor-imposed agreements. They thus reaffirm their interest in secrecy, rather than shifting responsibility to vendors.

In the absence of explicit provisions for overriding trade secrecy, and acknowledging the ineffectiveness in this domain of the right of explanation under AI Act art. 86, I argue that trade-secrecy claims in PP should primarily be contested based on the principle of legality in criminal law. Anti-circumvention arguments should also be refuted considering the static nature of the predictive variables typical of situational prevention (historic crime data and socio-economic descriptors), or markers like the unconscious behavioural components operationalised by 'Software A'. Variables of this type, essentially not alterable at the subject's will, make the risk of evasive strategies baseless. Upon closer inspection, challenging secrecy claims in general (whether 'trade secrecy' or 'anti-circumvention') essentially involves moving beyond a privacy-centred approach. Evidence of Its inefficacy is the GPDP investigation, which, despite precautionarily suspending 'Software B' in one municipality, was not deemed sufficient grounds for disclosing the markers to the public.

The 'privacy approach' is a core issue pervading all legal and political dimensions covered by the article. It reduces PP legality-assessment to the absence of natural persons' individual profiling at the output stage (a mere 'output-type' test), focusing solely on person-based PP as legally problematic. This makes both Italian systems admissible under the limited privacy/profiling-oriented ban of AI Act Article 5. This approach, well-illustrated by AI Act, Rec. 42, neither allows for the necessary distinction between two separate legal questions: on the one hand, the abstract legality of the type of software, which rests on permissive criteria; and on the other hand, the legality issues concerning the grounds of secrecy and the predictive variables themselves (regardless of the 'output test'). In this respect, the study has shown that 'Software A' raises fewer problems, given its reliance on behavioural descriptors serving only as connectors, rather than risk factors for future iterations. The issue with 'Software A', if any, lies in the programmatic endorsing of selective incapacitation theory. As for 'Software B', it incurs similar political concerns, with added concrete suspicions of unlawful predictive markers, considering public information

about both the criminological ideas prompting 'Software B' and other analogous systems whose markers have been disclosed. Concurrently, the company's persistent unresponsiveness, the investigation opened by the GPDP and the algorithm's suspension in one municipality, and the fact that the new GIOVE system will be modelled on 'Software A' technology do not support the legal conformity of the markers used by 'Software B'.

In summary, considering how intertwined PP is with the commercial origins of predictive analytics (Wilson, 2018) and the optimisation of policing harms (Benbouzid, 2019), the broader picture in Italy reveals a failure, for now, in making this market attractive. The commercial failure of the first version of Hunchlab in the US suggests that reorganisation phases are not exceptions and do not necessarily prelude definitive abandonments. The interlocutory stage in Italy also features an internal dialectic—with one company discrediting predictive mapping adopted by its competitor—and the advertising of fictional expansive trends. This unveils a deep concern not so much for public scrutiny, but for commercial image. However, this story is far from over, and an attempt for new proprietary software, GIOVE—with the approval of the DPS, yet at odds with EUCPN guidelines—is underway.

Using this case study, I argue for a regulatory approach that does not solely focus on the output type as the ultimate legality test. The currently dominant, 'profiling-centred' approach, modelled after privacy protection, neglects the power dimensions unique to law enforcement and equates PP with decision-making of a different nature (administrative or judicial). This article also emphasises that discriminatory effects may be easily embedded in the input data, regardless of the output appearance, and that the abstract lawfulness of the AI system type in no way justifies the secrecy of its predictive markers. Recognising the evolving nature of the situation and its regulatory framework, this study explores the factors at play in the Italian context, based on first-hand information, and lays the groundwork for further investigations. Future research could benefit from repeating this inquiry on a broader sample of companies and police agencies to identify developments in this evolving field and assess the real impact of the EU AI Act wherever it is binding law.

Annex 1

Table 1 'Software A'

Vendor	'Company A' (interviewed)
Tester	'HQ A'
Users	NO current users

Table 2 'Software B'

Vendor	'Company B' (non-respondent)
Testers	'Testers 1–6'
Users	'Users 1–21'

Table 3 'Software B': comparison between testing areas and declared areas of current use

	No. of areas	Total population	Average population per town	Total extension (km^2)	Average km^2 per town	Type of Police Force
Testing Phase	6 towns	5 342 294	890 382	15 106,81	2 517,80	National Police
Current users ('Company B' webpage)	21 towns	1 023 207	48 724	1 158,89	55,19	Local Police
Variations	+15 towns	- 80%	- 95%	- 92,33%	-97,8%	

Data source: Italian National Institute of Statistics (ISTAT)

Acknowledgements I express my gratitude to Fabio Chiusi, the Martorana Law firm, CILD (Civil Liberties in the Digital Age), and the Hermes Center for Digital Rights for their feedback during the early stages of my research. Additionally, I appreciate the participants who contributed to the study.

Author's contribution The author confirms sole responsibility for the study conception and design, data collection and analysis, and manuscript preparation.

Funding Open Access funding provided by University of Turku (including Turku University Central Hospital). The research leading to this article received funding from the University of Turku Graduate School until December 2023, the Turku University Foundation (Grant number 081436) between January and April 2024, and Suomalainen Lakimiesyhdistys (Apurahat v. 2023) from May 2024.

Data availability All original data generated in this research are available within the article.

Declarations

Ethical approval This study does not require ethical review based on the ethical principles of research with human participants and ethical review in the human sciences, established by the Finnish National Board on Research Integrity (TENK) guidelines 2019.

Informed consent Informed consent was obtained from all participants included in this study.

Statement regarding research involving human participants The study does not seek, collect or otherwise process personal data as defined by the Regulation EU 2016/679 (GDPR), focusing solely on information related to predictive technologies. Still, participant names, municipalities, and company details remain confidential.

Competing interests The author declares no competing financial or non-financial interests to disclose.

Table 4 'Software B': testers and current users ('Company B' webpage)

	Municipalities	Territorial extension km^2	Contribution to the research
Testing phase	Tester 1	365,66	confirms testing
	Tester 2	3.447,40	confirms testing
	Tester 3	2.687,88	non-respondent
	Tester 4	2.472,88	confirms testing
	Tester 5	4.954,05	confirms testing
	Tester 6	1.178,94	non-respondent
Current users	User 1	124.87	non-respondent
	User 2	37,14	non-respondent
	User 3	56,11	non-respondent
	User 4	59.85	non-respondent
	User 5	34,33	non-respondent
	User 6	152,81	confirms using
	User 7	42,13	denies using
	User 8	25,81	non-respondent
	User 9	4,73	non-respondent
	User 10	10.84	non-respondent
	User 11	6,21	non-respondent
	User 12	11,46	denies using
	User 13	117,77	non-respondent
	User 14	144,16	denies using
	User 15	43,66	denies using
	User 16	24,19	denies using
	User 17	71,60	denies using
	User 18	11,71	non-respondent
	User 19	6,87	denies using
	User 20	153,83	confirms using
	User 21	18,81	non-respondent

Data source: ISTAT

References

Algorace. (2025). Injustice by algorithm: 'Predictive' policing and criminal 'prediction' and profiling systems used by law enforcement and criminal justice authorities in Spain. Algorace & Statewatch. Accessed 26 November 2025. https://www.algorace.org/wp-content/uploads/2025/06/Report_Injustice-by-algorithm_JusticeandPolice-EN.pdf

Algorithm Watch (2020). *Automating Society Report 2020*. Accessed 26 November 2025. https://automatingsociety.algorithmwatch.org/

Alvesalo-Kuusi, A., & Whyte, D. (2018). Researching the powerful: A call for the reconstruction of research ethics. *Sociological Research Online, 23*(1), 136–152. https://doi.org/10.1177/1360780417747000

Babuta, A., & Oswald, M. (2019). *Data Analytics and Algorithmic Bias in Policing*. RUSI.Accessed 26 November 2025. https://assets.publishing.service.gov.uk/media/5d7f6b2540f0b61ccdfa4b80/RUSI_Report_-_Algorithms_and_Bias_in_Policing.pdf

Bachner, J. (2013). *Predictive policing. Preventing crime with data and analytics*. IBM Center for The Business of Government.

Baratta, A. (1989). Por una teoría materialista de la criminalidad y del control social. *Estudios Penales y Criminológicos*, *XII*(57), Servizo de Publicacións da Universidadede Santiago de Compostela, pp. 14–68.

Benbouzid, B. (2019). To predict and to manage. Predictive policing in the United States. *Big Data & Society*. https://doi.org/10.1177/2053951719861703

Bloch-Wehba, H. (2021). Visible policing: Technology, transparency, and democratic control. *California Law Review, 109*(3), 917–978.

Bradford, S., & Cullen, F. (2012). *Research and research methods for youth practitioners*. Routledge. https://doi.org/10.4324/9780203802571

Castigli, M. (2023). L'Italia fa già "polizia predittiva" ed è ad "alto rischio" ma non vietata dall'UE: ecco perché. *Cybersecurity360*. Accessed 26 November 2025. https://www.cybersecurity360.it/news/litalia-fa-gia-polizia-predittiva-e-ad-alto-rischio-ma-non-vietata-dallue-ecco-perche/

Couchman, H. (2019). *Policing by machine: Predictive policing and the threats to our rights*. London: Liberty. Accessed 26 November 2025. https://www.libertyhumanrights.org.uk/issue/policing-by-machine/

EUCPN. (2022). *Artificial intelligence and predictive policing: Risks and challenges*. EUCPN. Accessed 26 November 2025. https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf

Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*. Publications Office of the European Union. Accessed 26 November 2025. https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf

Fair Trials (2021). *Automating Injustice: the use of artificial intelligence & automated decision-making systems in criminal justice in Europe*. A ccessed 26 November 2025. https://www.fairtrials.org/articles/publications/automating-injustice/

Ferguson, A. (2017a). Policing predictive policing. *Washington University Law Review, 94*(5), 1109–1189.

Ferguson, A. (2017b). *the rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Galletta, A., & Cross, W. E. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication*. NYU Press.

Gatti, C. (2022a). Policing the poor through space: The fil rouge from criminal cartography to geospatial predictive policing. *Oñati Socio-Legal Series, 12*(6), 1733–1758. https://doi.org/10.35295/osls.iisl/0000-0000-0000-1360

Gatti, C. (2022b). Monitoring the monitors: A demystifying gaze at algorithmic prophecies in policing. *Justice, Power and Resistance, 5(*3), 227–248. https://doi.org/10.1332/UBQA2752

Gatti, C. (2023). The Bologna-Barcelona axis between Criminal Law Dogmatics and Critical Sociology of punitive control. Hidden Continuities and Apparent Overcomings. *Crítica Penal y Poder, 25*. https://doi.org/10.1344/cpyp.2023.25.44853

Gerstner, D. (2018). Predictive policing in the context of residential burglary: An empirical illustration on the basis of a pilot project in Baden-Württemberg, Germany. *European Journal for Security Research, 3*(2), 115–138.

Greenwood, P., & Abrahamse, A. (1982). *Selective incapacitation*. RAND Corporation.

Grossi, L. (2020). Software predittivi e diritto penale. In A. Massaro (Ed.), *Intelligenza Artificiale e Giustizia Penale*, 155–184. Accessed 26 November 2025. https://caterinachinnici.it/wp-content/uploads/2020/12/intelligenza-artificiale_ricerca.pdf

Hallevy, G. (2010). *A modern treatise on the principle of legality in criminal law*. Springer. https://doi.org/10.1007/978-3-642-13714-3

Harcourt, B. E. (2003). From the ne'er-do-well to the criminal history category: The refinement of the actuarial model in criminal law. *Law and Contemporary Problems, 66*(3), 99–151.

Harcourt, B. E. (2007). *Against prediction profiling, policing, and punishing in an actuarial age*. University of Chicago Press. https://doi.org/10.7208/9780226315997

Hulsman, L. H. C. (1986). Critical criminology and the concept of crime. *Contemporary Crises, 10*(1), 63–80. https://doi.org/10.1007/BF00728496

Joh, E. E. (2017). The undue influence of surveillance technology companies on policing, *NYU Law Review*, pp. 19–47. https://doi.org/10.2139/ssrn.2924620

Levano, J. (2024). Predictive policing in the AI Act: Meaningful ban or paper tiger? *European Law Blog*. Accessed 26 November 2025. https://www.europeanlawblog.eu/pub/tbgfjobj/release/1

Lorenz, L., Meijer, A., & Schuppan, T. (2021). The algocracy as a new ideal type for government organizations: Predictive policing in Berlin as an empirical case. *Information Polity, 26*(1), 71–86. https://doi.org/10.3233/IP-200279

Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Lynskey, O. (2019). Criminal justice profiling and EU data protection law: Precarious protection from predictive policing. *International Journal of Law in Context, 15*(2), 162–176. https://doi.org/10.1017/S1744552319000090

Manes, J. (2020). Secrecy and evasion in police surveillance technology. *Berkeley Technology Law Journal, 34*(2), 503–566. https://doi.org/10.15779/Z38NP1WJ7K

Millett, L. I., Lin, H. S., & Waldo, J. (2007). *Engaging privacy and information technology in a digital age*. National Academies Press. https://doi.org/10.17226/11896

Moore, T. (2017). *Trade Secrets & Algorithms as Barriers to Social Justice*. Center for Democracy and Technology. Accessed 26 November 2025. https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf

Morelli, C. (2019). Furti e rapine: a sventarli ci pensa l'intelligenza artificiale! Ecco i software di polizia predittiva utilizzati in Italia. *Altalex*. Accessed 26 November 2025. https://www.altalex.com/documents/news/2019/05/06/polizia-predittiva-intelligenza-artificiale

Neocleous, M. (2021). *A critical theory of police power: The fabrication of the social order*. Verso.

Neslen, A. (2021). Pushback against AI policing in Europe heats up over racism fears. *Reuters*. Accessed 26 November 2025. https://www.reuters.com/article/europe-tech-police-idINL8N2R92HQ/

Oosterloo, S. & Van Schie, G. (2018). The Politics and Biases of the Crime Anticipation System of the Dutch Police. In J. Bates (Ed.), *Bias. Proceedings of the Workshop on Bias in Information, Algorithms and Systems*, 30–41. Accessed 26 November 2025. https://ceur-ws.org/Vol-2103/

Parodi, C., & Sellaroli, V. (2019). Sistema penale e intelligenza artificiale: Molte speranze e qualche equivoco. *Diritto Penale Contemporaneo, 6*(2019), 47–71.

Pavoni, A., & Tulumello, S. (2023). *Urban violence: Security, imaginary, atmosphere*. Lexington Books.

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation. https://doi.org/10.7249/j.ctt4cgdcz

Platt, T. (1974). Prospects for a radical criminology in the United States. *Crime and Social Justice, 1*, 2–10. https://www.jstor.org/stable/29765882

Robinson, D., & Koepke, L. (2016). *Stuck in a Pattern. Early evidence on "predictive policing" and civil rights*. Upturn. Accessed 26 November 2025. https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf

Seidensticker, K., Bode, F., & Stoffel, F. (2018). *Predictive Policing in Germany*. Konstanzer Online-Publikations-System (KOPS). Accessed 26 November 2025. https://kops.uni-konstanz.de/server/api/core/bitstreams/10477c12-a4b9-46b2-b9d0-5b58cbd127bf/content

Taylor, I., Walton, P., & Young, J. (1973). The new criminology: For a social theory of deviance. *The New Criminology: For a Social Theory of Deviance.* Routledge.

Uchida, C. (2014). Predictive policing. In G. Bruinsma & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 3871–3880). Springer.

Weyembergh, A., & Galli, F. (2013). *Approximation of substantive criminal law in the EU: The way forward*. Éditions de l'Université de Bruxelles.

Wilson, D. (2018). Algorithmic patrol: The futures of predictive policing. In A. Završnik (Ed.), *Big Data, Crime and Social Control* (pp. 108–127). Routledge.