



# ‘We Attempted to Deliver Your Package’: Forensic Translation in the Fight Against Cross-Border Cybercrime

Rui Sousa-Silva<sup>1,2</sup>

Accepted: 22 December 2023 / Published online: 17 January 2024  
© The Author(s) 2024

## Abstract

Cybercrime has increased significantly, recently, as a result of both individual and group criminal practice, and is now a threat to individuals, organisations, and democratic systems worldwide. However, cybercrime raises two main challenges for legal systems: firstly, because cybercriminals operate online, cybercrime spans beyond the boundaries of specific jurisdictions, which constrains the operation of the police and, subsequently, the conviction of the perpetrators; secondly, since cybercriminals can operate from anywhere in the world, law enforcement agencies struggle to identify the origin of the communications, especially when obfuscation strategies are used, e.g. dark web fora. Nevertheless, cybercriminals inherently use language to communicate, so the linguistic analysis of suspect communications is particularly helpful in deterring cybercriminal practice. This article reports the potential of forensic translation in the fight against cybercrime. Although the term ‘forensic translation’ is typically understood as a synonym of ‘legal translation’, it is argued that the implications of forensic translation span beyond those of legal translation, to include analyses of language rights, of the right to interpretation and translation in legal procedures (in the EU), or even investigative and intelligence practices. Translation is a pervasive activity that is conducted, not only by professional translators, but also by lay speakers of language, often using machine translation systems. The ease of use of the latter makes it particularly suitable for cross-border criminal (e.g. extortion or fraud) and cybercriminal communications (e.g. cybertrespass, cyberfraud, cyberpiracy, cyberporn or child online porn, cyberviolence or cyberstalking). This article presents the results of the analysis of cybercriminal communications from a forensic translation perspective. It demonstrates that translation is frequently used to spread cybercriminal communications, and that reverse-engineering the translational procedure will assist law enforcement agencies in narrowing down their pool of suspects and, consequently, deter cybercriminal threats.

**Keywords** Forensic linguistics · Cybercrime · Language crimes · Translation studies · Translingual plagiarism

## 1 Introduction

Technology has long been part of the history of Humanity; ever since the early development of artefacts, humans have constantly produced new tools, methods, and techniques to make their daily tasks easier and communication more efficient. In language, this evolved from the invention of writing to the invention of the printing press, the telegram, and the telephone, all of which allowed communication worldwide, speedily and massively, first in written and then in spoken form. Technological progress followed by the massification of the Internet, which allowed billions of people worldwide to post messages systematically—in a way “that was previously confined to *mass media* and governments” ([31], p. 5). The massification of smartphones that followed grouped all these inventions and placed them in the hands of users ([31], p. 5). Consequently, the technological developments of the last decades have been particularly evident and have attracted general interest and attention, given the communication possibilities that technology has enabled and offered to common users.

Currently, anyone virtually anywhere is offered the possibility of communicating with practically anyone else instantly and multimodally. While the computer technologies used some decades ago allowed users with access to a computer and to the Internet to communicate via instant messaging services, the communication potential of these technologies was limited; not only was communication initially restricted to writing, but also instant messaging was far from being instantaneous, which sometimes originated minor or awkward misunderstandings, but often led to critical issues of miscommunication, including serious quarrels with interlocutors. This scenario changed dramatically over the last decades: as language technology has become more reliable and sophisticated, true real-time communication was enabled, which allowed users to employ a range of different modes, including text, voice, image, and video, simultaneously and instantaneously, and at a very low or no cost.

Technological developments, in general, and the developments in language technology, in particular, are likely to evolve even more significantly and faster in the near future. As hardware is powered with new capabilities, language technology will no longer be confined to mobile devices, but rather increasingly integrated with our senses [31]. This, in turn, offers more convenience, flexibility and accessibility, as users can now perform tasks on their phones via simple voice commands, get directions, ask about the weather, monitor traffic, and even use domotics to control home appliances, in addition to performing several other sophisticated tasks enabled by the Internet of Things (IoT). However, convenience and accessibility usually come at a cost, even if apparently technology is provided for free. One of the main and more critical costs is cybercrime.

Cybercrime has increased significantly in recent years, in no small part due to the technological advances of the last decades [41]. The massification of mobile devices, and the possibility of using those devices at almost any given time and place, has powered citizens to post and publish the information that they value the most [37] instantly. However, this widespread access to and use of connected

devices to exchange, publish and post whatever they like has also exposed users to more cybernetic attacks; new opportunities for cybercriminal practice emerged from this technological possibility which are explored by offenders. As more—and more sophisticated—technology is introduced, cybercriminals dedicate themselves to exploring three types of weaknesses: system, processes and user vulnerabilities. That is the case of the IoT. When they go online, users frequently expose themselves by sharing personal or identifying information (voluntarily or upon solicitation by a third party), or by failing to adopt safe procedures online, which makes them vulnerable to attacks. Additionally, these personal vulnerabilities are often exploited by attackers in combination with technical vulnerabilities, i.e., glitches in the technology that allow cybercriminals to gain illegal access to confidential information and often full control over the users' systems. Common examples of cybercriminal activities that result from the exploitation of these vulnerabilities include, among many others, identity theft, unauthorised access to confidential information, theft of credit card details, bank account details and financial information, and extortion.

As has been previously explained [37], one instance where both vulnerabilities were highly explored by cybercriminals was the worldwide lockdown due to the covid-19 pandemic. As the world gradually came to a shutdown just after the virus outbreak, social, educational, and professional activities that used to take place in-person had to move online, and this represented an overload for systems, including internet service providers, and software, in particular online meeting and streaming platforms. The need to quickly make available sufficiently robust systems to cope with the massive adoption of the online tools and resources required resulted in the launch of operational versions of software that had not been thoroughly tested. At the same time, the psychological strain placed on users to quick adapt to 'the new normal' life online allowed cybercriminals to explore those technological, procedural and user vulnerabilities [21, 29]. Although states all over the world have long ended general lockdowns due to the pandemic, a significant portion of activities that used to take place in person and moved online during the pandemic have remained online since, either for reasons of convenience, cost-effectiveness, or due to eco-friendliness. The high volume of online activities therefore remains a fruitful ground for cybercriminals, who continue to explore the vulnerabilities found in systems, processes, or users to prey on both individuals and organisations.

Unsurprisingly, cybercrime remains a threat to individuals, organisations, and democratic systems worldwide, and can be undertaken either by individuals, independently, or collectively, by organised and non-organised groups. Individual cybercriminal activities are usually undertaken by one person, typically a hacker, who acts on their own behalf for personal gain and out of their own motivation; cybercriminal activities undertaken collectively habitually target organisations, companies, or individuals based on their class characteristics. An example of the latter is ransomware, which consists of installing a type of cryptovirological malware in the victim's system and threatening to publish the victim's personal data, or permanently block access to—or destroy—the data (in this case, via cryptoviral extortion) until a ransom is paid. Although extensive research has been conducted, and measures have been adopted by national and international law enforcement agencies to combat it

[10, 41], the fight against cybercriminal threats and activities remains a serious challenge for law enforcement and legal systems worldwide, owing in particular to the very nature of cybercriminal threats and activities: they occur in cyberspace.

Firstly, because cybercriminals operate online, their threats and activities span beyond the boundaries of individual jurisdictions. Indeed, cybercrime is largely a form of transnational crime, as cybercriminals often operate from one country to prey on victims who may be located in different countries all over the world. This significantly constrains the investigation, policing and deterrence of those threats and activities, as well as the conviction of the perpetrators because, on the one hand the different layers of communication make it very difficult and complex to positively identify the offenders, and, on the other, legal cooperation across jurisdictions, at a transnational level, raises particular challenges to jurisdictions that are, in several instances, very difficult to overcome. Secondly, since cybercriminals operate in the cybernetic world—a world with no jurisdiction—, they have the potential to operate geographically from anywhere in the world, which gives them a competitive advantage over law enforcement. This, together with the sophisticated technological means that they use, including obfuscation strategies, dark web fora and stealth technologies, leads law enforcement agencies into struggling to identify the origin of the communications, or even to build a pool of suspects to investigate further. In fact, some of the tactics and strategies employed in the past by enforcement officers to override criminal systems used by criminals, such as traffic interception, GPS trackers and IP trackers, as well as standard methods like traditional undercover actions, have become obsolete by the increasing use of new obfuscation possibilities and heavily encrypted systems, such as the ones offered by the dark net.

Traditionally, cybercrime has been investigated based on computer forensics [33], notwithstanding the fact that cybercriminals tend to be at least one step ahead of law enforcement agencies: typically, cybercriminals resort to technological innovation when practising technology-enabled (online) crimes, and so they frequently have access to more sophisticated technology than police investigators. It is therefore reasonable to believe that, despite the advances in computer forensics, computational approaches alone are likely to have a very limited effectiveness in deterring cybercriminal offences. Conversely, linguistic analyses have an extraordinary potential to support the fight against cybercrime. This builds on the assumption that cybercriminals inherently use language to communicate, whether for purposes of extortion, fraud, ransomware, or other. Therefore, the linguistic analysis of suspect communications is particularly helpful in deterring cybercriminal practice, since it has the potential, not only to attribute authorship of a questioned, anonymous text, to one particular author from a pool of suspect authors, but also to establish the linguistic profiling of the anonymous author, in case a pool of suspects is absent. In this case, the forensic linguistic analysis has the potential to establish sociolinguistic features of the author(s) of the criminal text to determine the type of person who wrote the text based on the language that they use. Sociolinguistic profiling includes establishing whether the authors are native speakers of the language and, should that not be the case, determining their native language. This methodology is crucial in cybercriminal cases, because, as will be shown, a significant volume of cybercrime consists of cross-border criminal activities and is currently conducted transnationally.

Hence, since cybercriminal communications are typically formulated in one language and subsequently translated into the language of the respective jurisdiction, a forensic translation approach, which consists of a forensic linguistic analysis of the texts in combination with a detailed translational grounding, is required to fight against cybercrime. Moreover, as will be shown, language is resistant to the conscious control of the authors [7], who ignore its identifying potential.

This article thus presents the novel concept of forensic translation and discusses its potential for cybercriminal investigation and deterrence. In the following section, a definition of cybercrime is presented, followed by a discussion of linguistic analysis in cybercrime deterrence. The subsequent section makes the case for forensic translation. Next, three applications of forensic translation are presented: a case of translingual plagiarism detection and analysis, a case of sociolinguistic profiling, and an example of forensic translation, sociolinguistic profiling, and cybercrime.

## 2 Defining Cybercrime

Cybercrime can be briefly defined as a type of technology-enabled (online) crime, which has been treated over the years as traditional crime, with the exception that it takes place online. Wall [40], for example, proposes a typology of cybercrime consisting of four categories that replicate the traditional, offline types of crime: trespass, deception and theft, porn, and violence. Wall's typology, however, adapts these categories to reflect the characteristics of the online environment. The first of these is cyber-trespass, which includes trespassing ownership in online environments, such as unauthorised access to passwords, identity theft, or destruction of sensitive information. The second type of cybercrime is cyber-deception and cyber-theft, which consists of securing illegal access to information and materials online, including theft of intellectual property online and digital piracy. The third category is cyber-porn, which consists of illegally using pornographic contents, such as unauthorised use of nudity, sexual exploration (including child pornography), and the so-called 'revenge porn'. The last category, cyber-violence, incorporates activities that may cause physical and emotional trauma, or even death, including perjury, defamation and threatening online, dissemination of dangerous or harmful contents, harassment online, cyber-bullying and cyber-stalking, and incitement to hatred and violence by spreading hate speech.

In this sense, cybercrime has traditionally been considered as part of a virtual vs. real criminal practice binary, and hence a type of virtual crime that mimics and adapts reality, notwithstanding the fact that it cannot be considered to simply mimic the real; instead, activities taking place in the virtual world clearly have an impact on physical and geographic reality [16, 17]. A notable example of this impact is the case of sharing dangerous information and materials. Let us consider a case where cybercriminals share information online about how to produce improvised explosive devices (IEDs). If someone uses that information to materially produce a bomb and makes it go off, then sharing the illegal contents online cannot be considered to be simply an online activity, as the impact of the explosion will demonstrate. This clarification is crucial to address cybercriminal activities in all their complexity.

In the European Union, the Directorate-General for Migration and Home Affairs acknowledges that, as many types of traditional crimes, including terrorism, trafficking in human beings, drug trafficking, and child sexual abuse have either moved or are facilitated online, most criminal investigations require a digital component. Consequently, the European Union has designed laws and adopted actions that aim to improve the prevention and foster the investigation and prosecution of cybercrime, until now, with a focus on child sexual exploitation. For that end, the Union has adopted measures to promote capacity-building of law enforcement and the judiciary and encouraged work with the industry to empower and protect citizens.

In this context, the Directorate-General for Migration and Home Affairs of the European Commission defines cybercrime as “criminal acts committed online by using electronic communications networks and information systems”,<sup>1</sup> and emphasises that cybercrime is a borderless issue that can be structured into three categories: (a) crimes specific to the internet: this includes attacks against information systems, as well as spoofing and phishing activities, e.g. provision of fake bank websites to illegally obtain users’ personal data, notably usernames and passwords, and thus gain access to victims’ bank accounts; (b) online fraud and forgery: this category of cybercrime consists of large-scale fraudulent activities, which include, but are not limited to, identity theft, phishing, spam and malicious code; and (c) illegal online content: this category of cybercrime incorporates child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and hate speech, including glorification of violence, terrorism, racism, and xenophobia.

As cybercriminal activities have become more sophisticated, so have definitions of cybercrime been revised, as is understandable, given the need to address the cybercrime phenomenon in all its complexity. Thus, although the typology proposed by Wall over 20 years ago has made a significant contribution to understanding the intricate levels of cybercriminal practice, the nature of cybercriminal activities has changed and adapted to the new functionalities offered by technology, in particular language technology. In addition to the deployment of more robust systems to counter cyberattacks, and the cybercriminals’ successful attempts to override them, more immersive and accessible language technologies, offered across an increasing number of platforms, have made more communication possibilities available to users, and this, in turn, has not only offered more vulnerability opportunities for cybercriminals to explore, but has also converted common users of technology (typically, victims) into offenders.

Cybercriminal behaviour of this kind is largely encouraged by technology, since online interaction frequently gives users the impression that they are not interacting in the ‘real’ world, but instead somewhere in a virtual space that allows them to ‘hide’ behind a computer screen or smartphone, and consequently post, publish, comment, offend, harass, bully, or otherwise prevaricate in a way that most would be hesitant to do in instances of in-person, face-to-face communication. Additionally, online interaction is no longer limited by language boundaries. Whereas, in the

---

<sup>1</sup> Migration and Home Affairs, European Union, Cybercrime, available at [https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en), last accessed 16 October 2023.

past, users were only able to communicate in a language that they could speak, or at least understand minimally, current language technology, powered by sophisticated machine translation engines, allows users to communicate with anyone, even with other users that do not share the same language skills. This translation technology is not exclusive of online applications, and is also available for use in live, in-person contexts. For instance, anyone can use a smartphone app to record what their interlocutor is saying, transcribe their words, translate them to their own language, reply, translate the reply back to the interlocutor's language and play the reply so that the interlocutor can listen to it. Nevertheless, this technology is easier to use in online scenarios, as platforms (e.g. social media) allow the users to automatically translate the messages, posts and publications of users with whom they interact. The simple fact that this procedure is smoother and less awkward than the one required in face-to-face interaction encourages a higher degree of engagement and hence interaction between users. Consequently, language takes on a pivotal role, not only in monolingual, same language communication settings, but also in multilingual communication contexts. Thus, another layer of complexity is added to cybercriminal investigations, as technology moves from the means of committing cybercriminal activities to playing an active role in producing cybercriminal acts. This is a setting that law enforcement has so far overlooked, neglected, and/or underestimated.

Indeed, law enforcement agencies have traditionally (and understandably) focused on large-scale, highly critical cybercriminal activities, while backgrounding less critical, yet still serious offences against fellow citizens. Examples of these cybercriminal activities include the attacks described in Wall's 'cyber-violence' category, such as perjury, defamation and threatening online, dissemination of dangerous or harmful contents, harassment online, cyber-bullying and cyber-stalking, and incitement to hatred and violence by spreading hate speech. Although these activities are not at a level that may be considered as critical as, e.g., terrorism, their impact may be nefarious, as they have the potential to cause physical and emotional harm, trauma, or even death.

In this context, as has been argued, computer forensics has made a significant contribution to deterring cybercriminal activities, but this approach has been unable to address cybercrime to its full extent. While significant investments have been made in human, technical, training and financial resources to help law enforcement agencies combat cybercrime, an important aspect has been ignored: the analysis of language used by cybercriminals to communicate. It is a safe assumption that most instances of cybercriminal activity involve communication, and consequently, cybercriminals use language in their criminal practice. By doing so, offenders are unaware that language use enables their positive identification, much like, metaphorically speaking, a 'linguistic fingerprint'. As has been theoretically argued and empirically demonstrated [6, 13], every speaker of a language uses that language idiosyncratically, which distinguishes their use of language from how other speakers of the language use it. However, despite this potential, little attention has been paid to language in cybercriminal communications [38]: in many jurisdictions, forensic linguistic analysis has been scarcely used to provide evidence and/or assistance to the forensic investigation, and in jurisdictions where linguistic analysis has been considered in forensic contexts, its application to cybercriminal settings has been

insufficient, which is often due to the lack of awareness of the law enforcement community. Thus, although linguistic analysis of suspect communications is essential to deter cybercriminal practices, that application potential has been underestimated.

### 3 Linguistic Analysis for Cybercrime Deterrence

Language is commonly seen as a means that humans use to communicate. However, as Finegan [9] convincingly recalled, language is more than an arbitrary communication system; it is a system that speakers, writers and users of sign language explore with one aim, i.e. to do things, more than simply using it to announce, describe, or discuss things. Therefore, as they use language, speakers and writers “do things with words” [2]; they perform actions that would not otherwise be performed. This includes actions that typically bear a positive connotation, such as apologising, thanking, or congratulating, but, in cybercriminal contexts, language also has the power to threaten, harass, bully, or extort, among others. As Ainsworth [1] clearly put it, “language is the faculty more than any other that makes us human” (p. 30), and, thus, language use provides a clear reflection of whom the speakers or writers are. It is a shared principle among different linguistic theories that every speaker of a language has their own, unique way of using language, i.e. their own idiolect [6]. In other words, although speakers and writers of a specific community or country may learn a language from the same books, and vocabulary from the same dictionaries, their use of language is idiosyncratic, which means, as has been empirically demonstrated (see, e.g., [13]), that every speaker of a language makes a distinct use of that particular language.

Based on this theoretical, but empirically demonstrated principle, it is then possible to identify a speaker or writer by the language that they use. This is the main assumption underlying forensic authorship analysis, the branch of forensic linguistics that consists of analysing texts to establish, confirm, or discard a speaker or writer as the most likely author of a questioned text. Therefore, understanding language and how it works is the best practical way to draw theoretically sound conclusions from empirical analysis of texts, and, in cybercriminal contexts, positively identify the offenders by the language that they use.

Forensic linguistics, which consists of applying linguistic analyses in forensic contexts, has been a focus of research into linguistics, especially over the last four decades and particularly in English-speaking countries, although the area has meanwhile come of age across several other countries. The term ‘forensic linguistics’ has been used both in a narrow and in a broad sense, although some linguists prefer to use the term in the narrow sense, while saving the term ‘language and law’ to refer to forensic linguistics in a broad sense.

Therefore, in a broad sense, forensic linguistics usually subsumes three sub-areas: (i) the written language of the law; (ii) the study of interaction in the legal process; and (iii) language as evidence [7, 22]. Alternatively, some authors divide the discipline into the following three sub-areas: (i) the language of the law; (ii) the language of the court; and (iii) forensic linguistic evidence [12]. The International Association for Forensic and Legal Linguistics (IAFL) divides the discipline into

the following three sub-areas: (a) language and law; (b) language in the legal process; and (c) language as evidence.<sup>2</sup> The first of these sub-areas, language and law, includes approaches to legislation, comprehensibility of legal documents, analysis and interpretation of legal texts, study of legal genres, history of legal languages, legal discourse, multilingual matters in legal contexts, discourse analysis of legal resources, language and disadvantage before the law, language minorities and the legal system, language rights, power and the law, and intercultural matters and mediation in legal contexts. The second sub-area, language in the legal process, includes research and analysis of interviews with vulnerable witnesses, communicative challenges of vulnerable witnesses, police interviews, investigative interviewing, language testing of asylum seekers, bilingual courtrooms and second-language issues, courtroom interpreting, courtroom interaction, courtroom translation, courtroom language, police language, prison language, and language addressed to judge and jury in common and civil law courtrooms. Finally, the third sub-area, language as evidence, includes authorship analysis and attribution, analysis and detection of plagiarism, speaker identification and voice comparison, corpora compilation (e.g. statements, confessions, suicide notes), authorship profiling, consumer product warnings, trademark and contract disputes, defamation, product liability, deceptive trade practices, and copyright infringement.

The narrow definition of forensic linguistics restricts the discipline to the third sub-area only, language as evidence, i.e., to instances where linguistic analysis is used to assist the investigative or evidential process. By this token, forensic linguistic analysis is used both to assist law enforcement agencies in their investigation and to provide evidence in courts of law. However, forensic linguistic analyses are also common outside courts of law and law enforcement agencies. A notable example of this is its potential to assist universities in establishing whether someone has plagiarised.

In cybercriminal contexts, the sub-area that is of highest relevance is the third one, language as evidence (that is, forensic linguistics in a narrow sense). Linguistic evidence, in particular authorship analysis, sociolinguistic profiling, and analysis of disputed meanings, will assist law enforcement, both by providing useful information for the investigation, and by providing evidence in courts of law. By establishing the sociolinguistic profiling of anonymous authors, linguists conduct an analysis of the language used in those texts to provide some clues to the investigation regarding the type of sociolinguistic person that has written the text. Sociolinguistic profiling, which is distinct from psychological profiling, does not aim to determine the psychological state or characteristics of the authors of the anonymous texts, but rather to identify features in the text that can be used as an indication of some sociodemographic characteristics of the writer, including age group, level of education, socioeconomic status, sex/gender, geographical origin, or whether the author is a native speaker of the language, and, in case they are a non-native speaker, their native language. Sociolinguistic profiling is especially useful to the investigative process

<sup>2</sup> The International Association for Forensic and Legal Linguistics, Forensic Linguistics, available at <https://iafl.org/forensic-linguistics/>, last accessed 15 October 2023.

because it allows the investigators to narrow down the pool of suspects, when in the absence of specific suspects, and gear the investigation in the right direction.

Conversely, forensic authorship analysis is performed when the police have one or more suspects, in which case the linguist's task is to analyse the text(s) of questioned authorship (usually, anonymous or known to have been forged), alongside the texts whose authorship is known, and compare the samples to: (a) confirm that the text has been produced by a particular suspect; (b) discard one of the suspects as the possible author of the questioned texts; or (c) attribute the text to one author from a small set of authors.

Forensic authorship analysis is grounded on the principle of idiolect that, as speakers of a language, we make a distinctive use of the language that we all speak, and that use distinguishes us from other speakers. Hence, it is the forensic linguist's task to identify markers (i.e., patterns of the language used in the questioned texts) that are sufficiently discriminant, that is, features that reveal someone's writing style, and which are identifying of the most potential suspect. Methodologically, this requires the linguist to find patterns in the text that are used consistently in the texts of known authorship, and which are distinctive when compared to the patterns found in the texts written by the other suspects. A positive identification takes place when a set of patterns used consistently in the questioned document matches an identical set of patterns used consistently by one of the suspects. On the contrary, if one or more authors reveal stylistic patterns that are distinct from the questioned texts, it is likely that they are not the author(s) of the questioned texts. Forensic authorship analysis is thus crucial in cases of cybercriminal communications, e.g., to positively identify a suspect by the language that they use, and subsequently explain and justify their findings to support evidence-based decision-making.

Another application of forensic linguistics is the analysis of disputed meanings. Traditionally, criminals were known to use coded language to communicate, but over time, as the codes became easier to crack, communication among criminals became more sophisticated, subtle, and volatile. Additionally, although speakers of a language are trained to draw meaning from words from a very young age, in social contexts, meaning making is far more complex, and so is meaning understanding. Firstly, words frequently have several different meanings, represented by different entries in dictionaries. Therefore, the meaning drawn from such words does not necessarily match their predominant meaning. Secondly, in social interaction, it is frequent that meaning can only be inferred from the context, which requires an assessment of the interlocutors, the setting, the communicative situation, as well as aspects such as background and social distance, among other elements. A linguistic analysis built on principles of pragmatics is thus essential to establish, not only the communicative intentions of the interlocutors, but also the intended and/or face value meaning of the disputed text. The forensic linguistic analysis of disputed meanings is highly relevant, for instance, in cases of hate speech, defamation, cyber-bullying, or incitement to hatred, violence or terrorism.

Altogether, these three applications of forensic linguistics are crucial to investigating and giving evidence in cybercriminal cases. However, given the changes operated in cybercrime in recent years, which made it an increasingly transnational, cross-border issue, forensic linguistic analyses alone are likely to have a limited

impact on the investigative and evidential process; due to the use of translation methods and translation systems, traditional monolingual approaches to cybercriminal texts are no longer sufficient. Instead, a forensic translation approach is required.

## 4 The Case for Forensic Translation

Translation studies have been an area of research, including from the perspective of religions and subjectivities, from an early age, although most of those studies have theorised about translation [4]. In classical antiquity, for instance, Horace showed an interest in the concept of *fidus interpres* to discuss the principle of faithfulness. For him, a faithful translator is the one who renders the translation word for word, so as not to deviate from the original; a good translator is thus the one who is to be trusted, the one who does a timely job, to the satisfaction of both parties.

Later, St. Jerome shifted the focus of translation studies to the translation of the Bible. As this task revolved around an attempt to proceed with evangelisation, the translator was required to be faithful to the source language text, which contained the word of God. Therefore, little interference from the translator was to be expected, so the text was translated linearly and mechanically to the target language text, ideally establishing a match whereby one word in the source text would correspond to one word in the target text. As a result, at least in theory, anyone with access to a dictionary or to a word list should be able to translate the source text.

At a later stage, Schleiermacher shifted the focus to equivalence, and argued that this is a strategy to make sure that the translation is received in optimal conditions. The author believed that translation should enable the reader to have a gist of the language behind the original text, whereby 'oddness' in text resulting from the interlingual influence of the source text should be retained. In this sense, a translation should read like a translation to enable the reader to grasp the creative essence of the original text. Unlike previous approaches to translation theories, Schleiermacher argued that the translator had permission to take control over the text.

The fact that most of these classical translation theories focused on the translation of biblical or literary texts is not only apparent; traditionally, little attention has been paid by translation theories to technical and scientific translation, the translation of specialised language/ language for special purposes (LSP) texts, and these have to some extent encouraged and informed more contemporary translation theories [11].

Currently, translation of specialised language is a field of research on its own, with institutions worldwide promoting it. The European Union stands out as an example of those institutions: with 24 official languages (Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish), the Union states its aim to promote its cultural and linguistic diversity; hence, since the languages spoken in the different EU countries are part of the European cultural heritage, the EU attempts to support multilingualism not only in the work of its institutions and in its programmes, but also in its legal framework, including rules and regulations.

In tandem with these policies to support multilingualism across the member states, the Union has adopted several measures to legally protect EU citizens, no matter in which member state they are. Two examples are the Directive 2010/64/EU of the European Parliament and of the Council of 20 October 2010 on the right to interpretation and translation in criminal proceedings, and the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support, and protection of victims of crime. The two directives, although in a different way, grant citizens of the European Union the right to have access to translation and interpreting in criminal proceedings, regardless of the EU member state where they are and of their member state of origin. Similarly, EU citizens who are victims of crime have the right to be informed in their own language, wherever they are in the European Union.

Another salient example of the high importance of—and significant attention paid to—translation is the Court of Justice of the European Union (CJEU).<sup>3</sup> The CJEU is responsible for interpreting EU law so as to enforce its consistent application across all EU countries. The court typically settles legal disputes between national governments and EU institutions, but it can also be used by EU citizens, companies or organisations who feel that their rights have been infringed to take action against an EU institution. In order to ensure equal treatment and to guarantee that a call for action is interpreted appropriately, the court employs a large number of translators.

Both the CJEU and the directives 2010/64/EU and 2012/29/EU of the European Parliament and of the Council are examples of legal translation, i.e. the professional translation of legal texts. Translation and its sibling, interpreting, have long been applied in legal contexts, and hence they have been subject of in-depth research. The special nature of legal texts, their conceptual specificity, their linguistic and terminological complexity, their function, and the degree of accuracy that they require make legal translation particularly apt to be a field of enquiry on its own.

According to Šarčević [30], the need for legal translation has increased consistently over the years. This need, she admits, arises, to a large extent, from the need that legal professionals have of communicating across an increasing variety of multilingual and multicultural settings. Hence, legal translation, she argues, is “an act of communication across legal, language and cultural barriers enabling the law to function in more than one language at national, international, and supranational levels” (p. 187). However, if translation in general is extremely challenging, legal translation is even more so, not only because, as Šarčević argues, the translator is faced with the need to handle the “inherent incongruity of legal systems, cultures, and languages” (p. 187), but also because legal systems, which are aimed to reflect the moral values of the respective society, build upon systems of conceptualisation that are not always easy to convey in another language. Hence, since establishing equivalence between legal texts across different languages is nearly impossible, translators succeeding in doing so are sometimes believed to operate a miracle [18].

<sup>3</sup> Court of Justice of the European Union, available at [https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu\\_en](https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en), last accessed 20 October 2023.

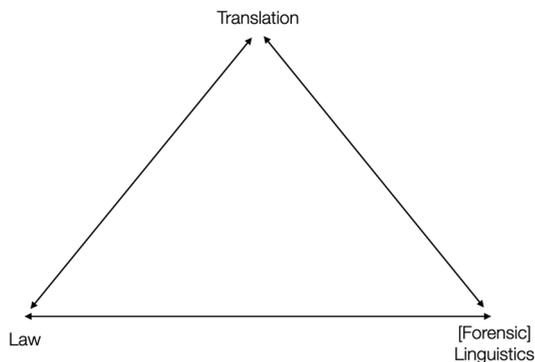
Šarčević rejects the need for the translator's ability to perform miracles; she builds upon Weigand's concept of 'terminological bridges' [42] to argue that all that translators need to perform a proper job as legal translators, and thus compensate for conceptual incongruity, is to have the legal expertise and the cultural sensitivity to use language effectively. This, of course, does not come without difficulties, including, among others: managing the approximation of versions of texts in different languages in multilingual jurisprudence, which has the potential to produce discrepancies between language versions and consequently jeopardise the uniform application of the law (as is notably the case of the one produced by the CJEU) [23]; understanding and accounting for the linguistic and cultural compromises involved in law making, and its inherent ambiguity [24]; choosing the more appropriate translation method, e.g. a teleological or a literal interpretive method [3]; understanding the concept of the translator's (in)visibility in legal translation [25]; or understanding the complexities of translating phraseology [28] or coerciveness in the court [5], among many others. Hence, legal translation implies a focus, not only on language, but also on terminology and on systems of conceptualisation.

Although legal translation and interpreting have been widely studied, even if from considerably different perspectives, most research has focused on the role of translation and translators in court settings, or of texts of legal nature, from the most theoretical and philosophical challenges to the operational difficulties. Conversely, little attention has been paid to translation in other legal settings, with the exception of interpreting in law enforcement contexts outside the courtroom, e.g. in police interaction [19] or unrepresented litigants in cases of small claims and private family proceedings [14]. However, the applications of specialised translation in forensic contexts span far beyond the court and police settings, and have an extraordinary potential as an investigative tool. This calls for a new term: 'forensic translation'. Forensic translation consists of applying translation studies, theories, knowledge, methods and techniques to forensic contexts, including for investigative and evidential purposes.

The concepts of legal translation and forensic translation share some features, including the aim of translating texts that have legal implications, and this explains why the two are often confused. However, they are different when analysed in detail. Contrary to legal translation, which can be circumscribed to the translation of legal texts (even if for judicial, normative, or informative purposes) or any texts to be used in the legal system, forensic translation applies to any text of virtually any type or genre for forensic purposes. One clear difference between the two is that legal translation handles documents such as proof of identity or contracts, among others, which have an inherently legal nature, but are of little interest for forensic translation; conversely, forensic translation has an interest in any document or communication that may be relevant for forensic purposes (although those documents or communications may not be of a legal nature, or may even be irrelevant for different legal systems).

The need for multilingual communication in legal settings has contributed to establishing a direct relationship between translation and the law (calling for legal translation), which demands competences and skills in translation, technology, service provision, in addition to personal and interpersonal skills, as well as

**Fig. 1** The tripartite model of forensic translation



cultural knowledge and, of course, language. Therefore, in this multidisciplinary scenario, linguistic and sociolinguistic competences and skills are only part of the translator's task, and not always the focus of attention.

Forensic translation, on the contrary, allows the expert to focus on the linguistic analysis of suspect, illegal, criminal, or otherwise immoral texts, supported by the theoretical and operational knowledge offered by translation studies, as well as by legal studies. Altogether, this framework allows the analyst to make theoretically grounded, and evidence-based conclusions about the nature, origin, or authorship of those questioned texts. Applications of forensic translation thus include, but are not limited to, providing assistance to analyses of language rights, monitoring the application of the right to interpretation and translation in legal procedures (in the European Union), forensic analysis of plagiarism, or to assist in investigative and intelligence processes, e.g. by analysing disputed meanings, attributing authorship of suspect texts, or establishing the sociolinguistic profiling of the authors of problem texts. The latter are common approaches to assist the investigation in cybercriminal communications. In summary, in forensic translation scenarios, the traditional bilateral relationship between translation and the law is replaced with a tripartite model, whereby a relationship is established between language and the law (forensic linguistics), law and translation, and translation and forensic linguistics. This tripartite model is illustrated in Fig. 1.

Similarly to forensic linguistics cases, which require the linguist to adopt a specific methodology from the 'linguist's toolkit' [7], depending on the nature of the case, in instances involving forensic translation, too, the choice of analytical methods is determined by the specifics of the case in point. Cases of forensic translation, specifically those involved in cybercriminal communications, typically share one feature: they tend to resort to machine translation.

Machine translation, which emerged in the mid-1940s, has evolved significantly since then: the rule-based machine translation approach that was initially adopted was later replaced by statistical machine translation, which subsequently gave way to hybrid machine translation systems. More recently, sophisticated machine translation systems have been developed which aim to simulate the brain

operations performed by translators when doing translation work (for a discussion about machine translation, see, e.g., [26]).

The development of sophisticated hardware, on the one hand, and software tools, on the other, has paved the way to entirely functional machine translated texts, which can be used for communicative purposes with little or no human intervention; that is to say that the quality offered by machine translation engines, regardless of whether it is identical to that offered by high quality, professional human translation [27], often suffices in many contexts where texts of less than perfect quality are enough to intermediate communication processes. This has encouraged the massification of machine translation systems, which are no longer limited to the knowledgeable use of professional translators, but, more importantly, are made available to any user, anywhere in the world, to translate virtually from and into any language.

The technical and financial possibility has offered general users, not only the perception that machine translation is of sufficiently good quality, but also the opportunity to communicate with anyone, anywhere in the world, regardless of their native language. As a consequence, machine translation has been used for all purposes, from socially praised activities (e.g. offering support in a language that users do not speak, or in which they do not feel fluent) to illegal action, e.g. for cybercriminal purposes, including extortion. Some of these actions, and how forensic translation approaches can be used to counter them, are discussed in the next section.

## 5 Applications of Forensic Translation

### 5.1 Translingual Plagiarism Detection and Analysis

One obvious application of forensic translation is plagiarism detection. Since plagiarism has traditionally been defined as taking someone else's words and passing them off as one's own, the phenomenon has commonly been approached as a same-language problem whereby the plagiarist would copy from another author's text in their language and then use it, partially or entirely, as their own work. This concept of plagiarism has been predominant for a long time, so measures to prevent, detect, and punish plagiarists have unsurprisingly focused on monolingual texts. However, more recently, in no small part due to the developments in machine translation, plagiarists have taken a text written by someone else in another language, (machine-) translated it into their native language (or the language in which they were supposed to write) and pass it off as their own [36]. This type of plagiarism has been termed 'translingual plagiarism' [34, 35].

Detecting translingual plagiarism is challenging because the so-called (although mistakenly) 'plagiarism detection' tools usually fail to detect this form of plagiarism as the plagiarised text (i.e., the original text) and the plagiarising text (i.e., the inappropriate textual reuse) are not in the same language. Since a direct algorithmic comparison cannot be established, detecting and analysing this form of plagiarism requires a distinct method. It is a well-known assumption that the tools that are used by plagiarists to plagiarise can also be used to find plagiarism [7]. In the case of translingual plagiarism detection, this involves a process of reverse engineering: if

one builds on the assumption that plagiarists typically plagiarise out of either laziness or lack of time, then it is evident that, when copying from other languages, plagiarists will neither translate the texts themselves, nor resort to professional translators; on the contrary, it is more likely that they use one of the freely available machine translation engines to translate into the target language and pass the text off as their own, after introducing minor or major alterations.

It is worth noting that machine translation engines do not all perform equally well; rather, the quality of their output depends largely on the language pair, the text type, the text genre, the text domain, and the writing style. In addition, machine translation systems tend to perform relatively well when translating vocabulary, but their performance tends to drop (often, abruptly) when the syntax is more complex or strikingly different from the one in the source language. Let us take, for instance, English and Portuguese. When translating between the two languages in the pair, machine translation tools tend to perform relatively well when translating vocabulary, but the typical Portuguese syntax is far more complex than the English, as it allows, for instance, embedding clauses in other embedded clauses unambiguously, without missing the sentence meaning. Additionally, unlike English, the Portuguese morphology allows gender and number inflection, which makes the referent clear in instances of complex sentences containing embedded clauses and reference structures. Both these features of the Portuguese grammar are extremely challenging for machine translation systems. Conversely, when the syntax of the two languages is closer (e.g. because they are part of the same language family), machine translation systems tend to show better performance rates. Knowledge of these differences, which translators or linguists familiar with translation command, will provide important background details to handle cases of translanguing plagiarism: (i) if a sentence in one language reads awkward and is reminiscent of a sentence typical of another language, it may be the result of translanguing plagiarism; (ii) if a sentence shows a syntactic structure that is oversimplistic and untypical of the language, it may be the result of machine translation from a less syntactically complex language.

Let us consider the following illustrative example: in a class assignment, a group of students submitted a text containing the following sentence:

*Os procedimentos são baseados no corpo geralmente aceite de conhecimento e experiência no campo da examinação de documentação forense.*

A reader of Portuguese will find that some of the elements in this sentence are awkward or odd: (i) the use of the passive voice, though grammatical, is far less commonly used in Portuguese; (ii) the position of the adverb 'geralmente', despite being grammatical in Portuguese, is highly marked, and thus infrequent; (iii) the collocation of 'corpo' + 'conhecimento e experiência' is uncommon—i.e., the phrase 'corpo de conhecimento' is acceptable, but not 'corpo de experiência'; and (iv) the choice of the word 'examinação', albeit lexicographically permitted, is used far less frequently than its unmarked equivalent, 'exame' or (perhaps even better) 'análise'. Altogether, these elements, which act as indices of foreignness, offer the reader the impression that the sentence reads like English.

Therefore, in cases where the reader may be suspicious of plagiarism, it suffices to reverse-engineer the suspect text, by machine translating the text into the most

**Table 1** Illustrative example of translingual plagiarism

PT	<i>Os procedimentos são baseados no corpo geralmente aceite de conhecimento e experiência no campo da examinação de documentação forense</i>
PT-EN	<b><i>The procedures are based on generally accepted body of knowledge and experience in the field of forensic documentation examination</i></b>
EN	<b><i>The procedures outlined here are grounded in the generally accepted body of knowledge and experience in the field of forensic document examination</i></b>

likely language of the original, and then performing a search online to investigate whether a version that is similar or identical to the machine translated version is available. Table 1 illustrates this process. The first column shows the language of the text: 'PT', in the first line, shows the sentence submitted by the students, in Portuguese; 'PT-EN', in the second line, shows the machine translated version of the text from Portuguese to English. The third line, 'EN', shows the original, plagiarised English text (the overlapping text in the machine translated version and the original, source text is shown in bold italics):

The comparison of the text of the second line, 'PT-EN', with the text of the third line, 'EN', shows an extremely high degree of similarity, as the overlapping text (in bold italics) shows. Only two words in the machine translated version shown in the second line are not part of the original, plagiarised version in the third line ('based' and 'on'), and only one word is slightly different, due to the addition of the suffix 'ation' in 'documentation'. All other words in the machine translated version are identical to those in the original version of the text, in English. The minor differences, in this case, result from the changes made by the plagiarists as they attempted to disguise the lifting, or from the challenges faced by machine translation engines to resolve ambiguities during the translation process.

This method is typically used to detect and analyse cases of plagiarism, but it is sufficiently robust to also enable the analysis of any instance of illicit textual overlap across two or more different languages, or even to investigate instances of English-based, machine-generated text.

## 5.2 Sociolinguistic Profiling

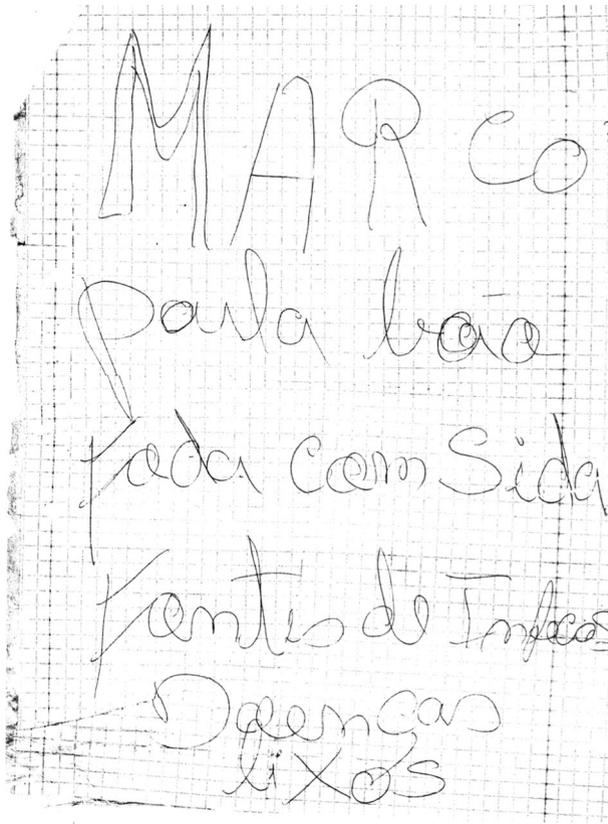
Forensic linguistic analyses of authorship typically build upon two solid theoretical linguistics principles: dialect and idiolect. Whereas idiolect, as mentioned earlier, builds upon the theoretical assumption that each speaker of a language has their own, idiosyncratic way of speaking or writing [6], the term dialect is used to refer to the variation observed in the use of language by speakers or writers of the same language that are separated geographically or socially [9]. Although the phenomenon of language variation has been extensively studied in linguistics, and particularly by linguists with an interest in sociolinguistics [15, 20, 39], the concepts have been retrieved by forensic linguists to address specific challenges in current society. One of the applications of the analysis of language variation in forensic contexts is sociolinguistic profiling.

Sociolinguistic profiling is usually treated by forensic linguists as a form of forensic authorship analysis [8]. However, whereas the most common authorship analysis task, authorship attribution, typically involves establishing the most likely author of a questioned text, from a closed set of possible authors, in cases of authorship profiling, neither the linguist, nor the investigation have any cues about the possible author(s) of the problem text. The role of the linguist, in these cases, is then to analyse the text and find linguistic evidence to establish what type of linguistic person wrote the questioned text, and so allow the investigation to narrow down the pool of suspects. The forensic linguist is thus tasked with finding information, based on the language used in the text, about the age group of the author, their sex and/or gender, their level of education, their social background, and whether they are a native or non-native speaker of the language and, in the case of the latter, what their native language is. Therefore, in addition to having an excellent command of dialectal features, linguists involved in sociolinguistic profiling are also required in-depth knowledge of forensic linguistic analysis and an extensive understanding of translation, including cross-linguistic theories, interlanguage, and contrastive linguistics.

Sociolinguistic profiling tasks, however, are very challenging, as they require the acknowledgement of some crucial features. Firstly, some sociolinguistic categories, such as gender, are very difficult to establish. Legal and law enforcement systems operate largely based on the male/female biological binary, which corresponds to sex, but gender, as a social category, is more fluid and hence the distance between different gender categories, including transsexual individuals, is typically more problematic to determine linguistically. Secondly, language is pervasive across time and space, but this pervasiveness is subject to change. Consequently, language use by each speaker and writer is expected to vary, not only diachronically, over time (e.g., as they grow older), but also geographically (diatopic variation), according to their social class or to the social group with which they identify themselves (dias- tratic variation), and according to the setting (diaphasic variation). Thirdly, speakers and writers of a language are permanently in social contact with other speakers and writers of the language, which results in their accommodating to the context and/or to the interlocutors, e.g., by adopting linguistic features of the latter. Altogether, these elements make it more challenging for forensic linguists to establish the sociolinguistic profile of the suspect with absolute certainty.

In cybercriminal cases, the difficulty of the profiling task is furthered by the fact that society, and thus cybercrime, are increasingly cross-lingual and multilingual due to globalisation, while identities become more fluid and individual profiles increasingly complex. Unsurprisingly, therefore, translation turns into a ubiquitous activity that is performed, not only by professional translators, but also by lay (untrained) speakers and writers, by machines or even, as has been witnessed more recently, by generative artificial intelligence models. These systems are used for different purposes, including transnational cybercriminal practice and communications (such as, among others, cybertrespass, cyberfraud, cyberextortion, cyberpiracy, cyberporn or child online porn, cyberviolence, or cyberstalking). These complexities call for a translanguing, forensic translation approach as part of sociolinguistic profiling.

Figure 2 shows a handwritten message which was part of a case of cyberstalking investigated by the Cybercrime Office of the Portuguese Prosecutor's Office. In

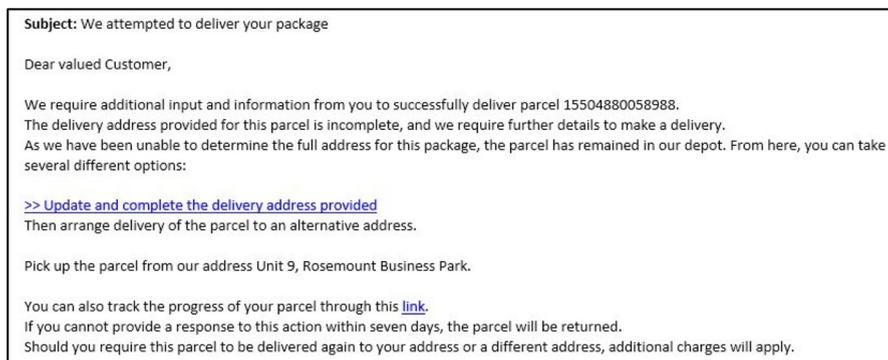


MARCO  
 Paula baõ  
 fada com Sida  
 fontes de Infec  
 Doenças  
 liXOs

**Fig. 2** A case of sociolinguistic profiling

addition to the handwritten message, short text messages were sent from two different prepaid and unregistered mobile phone numbers spreading defamatory contents. The aim of the linguistic analysis was twofold: (1) to check whether the language used across the three sets of texts (messages sent from the two mobile phone numbers and the handwritten note) was consistent, and therefore whether the same author had written the texts; and (2) to subsequently establish the sociolinguistic profiling of the author, as a means to narrow down the pool of suspects.

Although the amount of text available for linguistic analysis is very small (448 words in one set of SMS messages, 122 words in the other set, and 16 words in the handwritten message), the analysis revealed that the three sets share numerous atypical linguistic patterns, including slang and swear words, lack of punctuation (especially at the end of sentences), lack of accents in words, lack of prepositions, missing trailing spaces between words, homophonic substitution (i.e., the correct spelling is replaced by how the words are pronounced), spelling errors, and lack of gender and number agreement, as is required by Portuguese grammar). The messages also include an idiosyncratic phrase that is made highly idiolectal by the use of



**Fig. 3** Fraudulent message (in English)

the wrong preposition: ‘homem de sida’ (literally translated into English as ‘man of aids’ to mean ‘man with aids’).

Given the idiosyncratic features shared across the three sets of text, it is highly likely that the author of the three sets is the same. Additionally, the analysis of the patterns found offers several sociolinguistic cues to the origin and social characteristics of the writer, who is highly likely to be a woman in her mid-20s to mid-30s, with a low level of education, and from a low socioeconomic background. The linguistic patterns observed in the analysis also suggest that the writer, most probably a black woman, originates from a Portuguese-speaking African country, probably Angola or, even more likely, São Tomé and Príncipe. Additionally, those patterns also have a significant potential to help narrow down the pool of suspects.

In cases of sociolinguistic profiling, linguists usually interpret their findings with caution because, as mentioned earlier, language is fluid, and although different social groups tend to share stable intra-group sociolinguistic patterns, which differ from inter-group patterns, some features may span beyond the borders of individual groups and be used by individual members of other groups.

### 5.3 Sociolinguistic Profiling and Cybercrime

The principles employed for establishing the sociolinguistic profile of the authors can also be applied to the investigation of cross-border cybercriminal practice. Figures 3 and 5 (written in English) and 4 and 6 (written in Portuguese) illustrate an example of fraudulent and deceptive messages sent to citizens for purposes of extortion.

In the two messages, the addressee is informed that a package could not be delivered to them because the delivery address is missing or is incomplete. The recipient is then asked to act, by providing the details required for the successful delivery of the parcel. Information is also provided on how the addressee can track the parcel. This, together with the fact that the information about the local parcel service is localised (i.e., adapted to the locale of the recipient) increases the credibility of the message, in the eyes of the inattentive recipient.

Caro Consignatário,

Para procedermos à entrega da encomenda número RD463746354PT, precisamos da sua intervenção.  
O endereço de entrega fornecido para esta encomenda está incorreto ou não existe, uma vez que os nossos estafetas não conseguiram chegar a este local.

Uma vez que esta tentativa de entrega não foi bem-sucedida, a sua encomenda foi devolvida ao nosso armazém.  
A partir de agora, pode escolher várias opções diferentes:

[>> Atualizar o endereço de entrega fornecido](#)  
>> [Agendar a entrega da encomenda num endereço alternativo](#)

Pode também acompanhar o progresso da sua encomenda através deste link.  
Se não conseguir responder num prazo de dois dias, esta encomenda será devolvida ao remetente original.  
Dependendo do tipo de encomenda, o remetente poderá ter de pagar taxas de devolução.

Poderá, também, recolher a encomenda no nosso armazém em Merc. For Do Tijolo Lj 16 A 18, 1170-221.  
A nova entrega desta encomenda está sujeita ao pagamento das taxas que se encontram detalhadas nos links supra indicados.

Com os melhores cumprimentos,  
CTT  
[www.ctt.pt](http://www.ctt.pt)  
*Esta mensagem é enviada automaticamente, por favor não responda.*  
*Em caso de dúvidas ou informações adicionais, aceda a [www.ctt.pt/ajuda](http://www.ctt.pt/ajuda)*

**Fig. 4** Fraudulent message (in Portuguese)

A close scrutiny of the two messages shows that, with the exception of the language used (English, in the one shown in Fig. 3, and Portuguese, in the one shown in Fig. 4), they are very identical in structure and contents. Furthermore, the linguistic formulation, though not perfect, is fully functional, contrary to the basic, oversimplistic, and grammatically incorrect language employed in the deceptive messages that used to be spread in the past. Therefore, since the quality of the language currently used in deceptive messages has improved, when compared to those spread in the past, recipients can no longer rely on the low quality of the language as cues to deception. As a consequence, the deceptive potential of these messages is nowadays comparatively higher.

Similarly, Figs. 5 and 6, which are from a case of attempted ransomware, are used to inform the recipient that they have been video recorded watching porn on their computer screen and warn them that, unless they transfer a significant sum to a bitcoin account, the video recording will be publicly disseminated. The message includes important coherence information, which could point to its deceptive nature: (i) it implies that the recipient has two screens, which is of course not always the case; and (ii) it states that the recipient has been watching porn, a piece of information whose truthfulness the victim will know better than anyone else. Obviously, these are aspects that the recipient may overlook, not the least because they may believe that the offenders might edit real videos with the intent to falsely accuse them. Linguistically, the two messages reveal identical structural patterns and only minor language issues (which most probably result from machine translation errors) that are highly likely to pass unnoticed to most recipients.

The two cases illustrated in messages 3 and 4 and 5 and 6 suggest that cybercrimes like extortion and ransomware—which are ‘language crimes’ [32], as they are, to a significant extent, committed through the use of language—are largely dependent on machine translation. The pervasiveness of machine translation engines enables any cybercriminal operating from anywhere in the world to

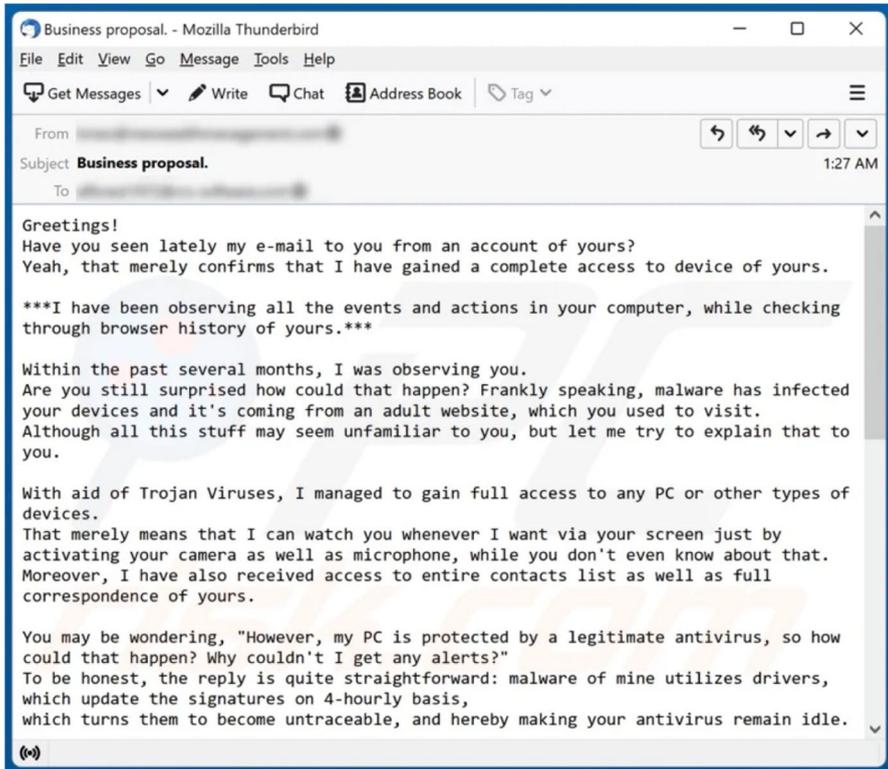


Fig. 5 Ransomware message (in English)

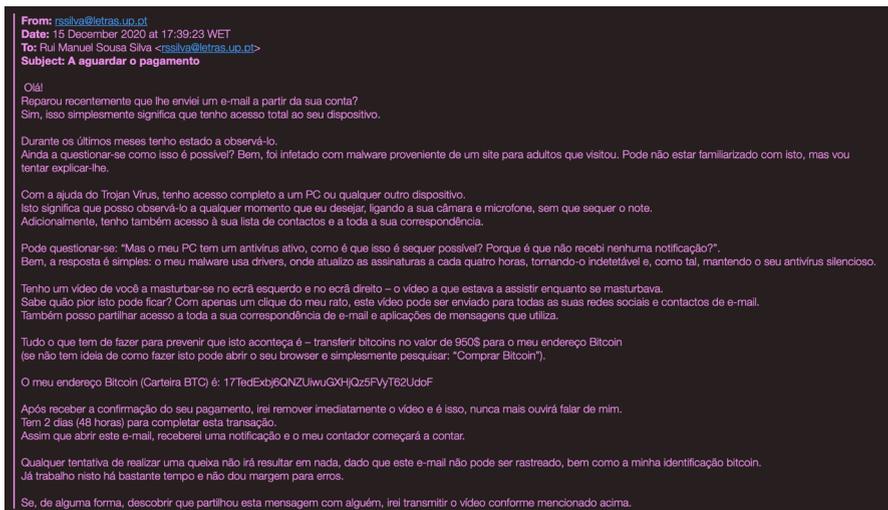


Fig. 6 Ransomware message (in Portuguese)

act transnationally, and hence impose criminal offences upon victims that may be geographically distant, or even located in another jurisdiction. More importantly, the sophistication of those engines enables cybercriminals to spread their offences, even when they cannot speak the native language of the victims.

In this context, forensic translation approaches are doubly helpful: on the one hand, the identification of the patterns used in cybercriminal communications will enable national and international authorities to inform citizens about how to protect themselves from these cybercriminal attacks (companies worldwide have tried to inform their customers about those cybercriminal offences, but the fact that they show mostly illustrative examples, in addition to the fact that the form of the messages changes with the technological developments, curtail the effectiveness of the campaigns); on the other hand, the detail retrieved from forensic translation analysis not only enables states to adopt counter-cybercriminal systems, but also assists law enforcement agencies in establishing the sociolinguistic profiling of the offenders, notably the origin of the attacks, and eventually contributes to bringing them to justice.

The field of forensic translation is a promising field of research, despite its facing two main challenges that arise from technological developments: machine translation (MT) and generative artificial intelligence (AI). As machine translation systems evolve, the quality of translation output improves, and even if that quality may, in many instances, fall short of the quality of translation produced with human intervention, it is likely that MT systems are increasingly and successfully used for deceptive purposes. The same applies to text generated by artificial intelligence: although AI-generated text appears to be good on the surface, closer scrutiny shows that it is flawed with linguistic imperfections, as preliminary empirical observation demonstrates. Therefore, despite the likelihood that such flaws are overlooked by lay users of the language, they currently fail to pass unnoticed to trained linguists. Nevertheless, the training of new large language models is likely to enable artificial intelligence to mimic text produced by humans more competently, which in turn will make it more difficult to distinguish between AI- and human-generated text. Moreover, generative pretrained transformer (GPT) systems are increasingly integrated with MT systems, thus adding another layer of complexity to the forensic linguistic and forensic translation analysis. Given the nature of current language technology, any forecast is largely speculative. However, if one considers the very nature and complexity of human language, including biological features involved in language production such as homeostasis, in principle linguistic analysis will remain of essence in establishing the difference between AI- and human-generated text. However, research into forensic translation will need to be furthered so as to remain a step ahead—rather than keep up with—the rapidly changing language technology. This is especially the case in cybercriminal scenarios.

## 6 Final Remarks

The term ‘forensic translation’ has been used infrequently. However, on the occasions in which it has been used, the term has been employed as a synonym of ‘legal translation’. Although the two terms share the fact that they can be used in and by the courts (the *forum*, in the traditional sense), in this article I have argued for the need to make a clear distinction between the two. Whereas legal translation is restricted to translating texts related to legal issues and to the courts, forensic translation should be used more broadly to include all applications where translation theories, methods, and techniques can assist the courts, law enforcement agencies, and organisations in general in enforcing lawful, ethical, and moral practices and standards. Forensic translation can thus be defined as the interdisciplinary branch of forensic linguistics that applies knowledge and expertise of translation in forensic contexts. To support this claim, three illustrative examples have been presented that demonstrate the relevance of forensic translation: (i) translanguing plagiarism detection and analysis; (ii) sociolinguistic profiling; and (iii) cybercrime detection and deterrence.

The analysis of the data and the subsequent discussion show that machine translation is increasingly used and employed more pervasively, both by the general population, and by cybercriminals; hence, as technological developments allow for more high-quality translation systems, cybercriminal communications are likely to become more sophisticated, and hence it will become comparatively more difficult to distinguish between deceptive and genuine communications. In this context, it has been argued, further developments in forensic translation analyses will enable legal, law enforcement, and official institutions to devise appropriate methods and systems to ensure the safety and security of citizens, and eventually reinforce democratic systems, in full respect for subjectivities, religions, and freedom of choice.

The relevance of the field of forensic translation is bound to increase in the future. With the technological developments in artificial intelligence (AI) systems, cybercriminals will be able to multiply their attacks, while doing so at a higher speed, by machine-generating text at a rate that is humanly impossible. Therefore, generative AI systems, which are trained on large language models (LLMs) built mostly for English, in combination with increasingly powerful and sophisticated machine translation systems, will offer offenders unprecedented opportunities for cybercriminal practice across jurisdictions, transnationally. In this setting, forensic translation approaches will have the potential to combine the ability to distinguish text produced by humans from text produced by machines, while sociolinguistically profiling the text producer. Research is already underway in this direction.

**Acknowledgements** I would like to thank the anonymous reviewers for their positive feedback and, in particular, for their comments and suggestions, which certainly contributed to an improved version of this article.

**Funding** Open access funding provided by FCTIFCCN (b-on). Fundação para a Ciência e a Tecnologia, UID/00022/2020.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Ainsworth, J. 2021. How I got started. *Language & Law/Linguagem e Direito* 7 (1–2): 30–32.
2. Austin, J.L. 1962. *How to do things with words*. Oxford: Clarendon Press.
3. Baajji, C.J.W. 2012. Fifty years of multilingual interpretation in the European Union. In *The oxford handbook of language and law*, ed. P.M. Tiersma and L.M. Solan. Oxford: Oxford University Press.
4. Bassnett, S. 2002. *Translation studies*, 3rd ed. London: Routledge.
5. Berk-Seligson, S. 1999. The impact of court interpreting on the coerciveness of leading questions. *International Journal of Speech, Language and the Law* 6 (1): 30–56. <https://doi.org/10.1558/sll.1999.6.1.30>.
6. Coulthard, M. 2004. Author identification, idiolect, and linguistic uniqueness. *Applied Linguistics* 24 (4): 431–447.
7. Coulthard, M., and A. Johnson. 2007. *An introduction to forensic linguistics: Language in evidence*. London: Routledge.
8. Coulthard, M., and Sousa-Silva, R. 2016. Forensic Linguistics. In *What are Forensic Sciences? – Concepts, Scope and Future Perspectives*, ed. R. J. Dinis-Oliveira, and T. Magalhães, 137–144. Pactor.
9. Finegan, E. 2008. *Language: Its structure and use*, 6th, Inter ed. Boston: Wadsworth.
10. Forte, E., T. Schotte, and S. Strupp. 2017. *Serious and organised crime in the EU: The EU Serious and Organised Crime Threat Assessment (SOCTA) 2017*. 16.
11. Gentzler, E. 2011. *Contemporary translation theories*, 2nd ed. Clevedon: Multilingual Matters.
12. Gibbons, J., and M.T. Turell, eds. 2008. *Dimensions of forensic linguistics*. Amsterdam: John Benjamins Publishing.
13. Grant, T. 2021. Text messaging forensics—Txt 4n6: Idiolect-free authorship analysis? In *The Routledge handbook of forensic linguistics*, 2nd ed., ed. M. Coulthard, A. May, and R. Sousa-Silva, 558–575. New York/London: Routledge.
14. Grieshofer, T. 2022. The importance of being heard: Stories of unrepresented litigants in small claims cases and private family proceedings. *Language and Law/Linguagem e Direito* 9 (1): 73–91. [https://doi.org/10.21747/21833745/lanlaw/9\\_1a4](https://doi.org/10.21747/21833745/lanlaw/9_1a4).
15. Guy, G. 1980. Variation in the group and the individual. In *Locating language in time and space*, ed. W. Labov, 1–36. New York: Academic Press.
16. Holt, T.J., and A.M. Bossler. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35 (1): 20–40. <https://doi.org/10.1080/01639625.2013.822209>.
17. Holt, T.J., and A.M. Bossler. 2016. *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge.
18. Kjær, A.L. 2008. The every-day miracle of legal translation: Deborah Cao: Translating law (Clevedon, Buffalo, Toronto: Multilingual Matters 2007), 189 pp, ISBN-13: 978-1-85359-954-5 (= Topics in Translation 33). *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique* 21 (1): 67–72. <https://doi.org/10.1007/s11196-007-9057-x>.
19. Kredens, K., E. Monteoliva-Garcia, and R. Morris. 2021. Interpreting outside the courtroom: 'A shattered mirror?' Interpreting in law enforcement contexts outside the courtroom. In *The Routledge handbook of forensic linguistics*, 2nd ed., ed. M. Coulthard, A. May, and R. Sousa-Silva, 502–520. London/New York: Routledge.
20. Labov, W. 1972. *Sociolinguistic patterns*. Philadelphia: University of Pennsylvania Press.

21. Lallie, H.S., L.A. Shepherd, J.R.C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens. 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security* 105: 102248. <https://doi.org/10.1016/j.cose.2021.102248>.
22. May, A., Sousa-Silva, R., and Coulthard, M. (2021). Introduction. In *The Routledge handbook of forensic linguistics*, 2nd ed., ed. M. Coulthard, A. May, and R. Sousa-Silva, 1–8. New York/London: Routledge.
23. McAuliffe, K. 2013. The limitations of a multilingual legal system. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique* 26 (4): 861–882. <https://doi.org/10.1007/s11196-013-9314-0>.
24. McAuliffe, K. (2014). Translating ambiguity. *Journal of Comparative Law* 9 (2). <https://doi.org/10.5771/9783748927884-251>.
25. McAuliffe, K. 2016. Hidden translators: The invisibility of translators and the influence of lawyer-linguists on the case law of the court of justice of the European Union. *Language & Law/Linguagem e Direito* 3 (1): 5–29.
26. Mitkov, R., ed.. 2022. *The Oxford handbook of computational linguistics*, 2nd ed. Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780199573691.001.0001>.
27. Mossop, B. 2020. *Revising and editing for translators*, 4th ed. Abingdon: Routledge.
28. Ruusila, A., and E. Lindroos. 2016. *Conditio sine qua non: On Phraseology in Legal Language and its Translation. Language & Law/Linguagem e Direito* 3 (1): 120–140.
29. Saleous, H., M. Ismail, S.H. AlDaajeh, N. Madathil, S. Alrabae, K.-K.R. Choo, and N. Al-Qirim. 2023. COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks* 9 (1): 211–222. <https://doi.org/10.1016/j.dcan.2022.06.005>.
30. Šarčević, S. 2012. Challenges to the legal translator. In *The Oxford handbook of language and law*, ed. P.M. Tiersma and L.M. Solan. Oxford: Oxford University Press.
31. Sayers, D., Sousa-Silva, R., Höhn, S., Ahmedi, L., Allkivi-Metsoja, K., Anastasiou, D., Beňuš, Š., Bowker, L., Bytyçi, E., Catala, A., Čepani, A., Chacón-Beltrán, R., Dadi, S., Dalipi, F., Despotovic, V., Doczekalska, A., Drude, S., Fort, K., Fuchs, R., ... Yildirim Yayilgan, S. 2021. *The Dawn of the Human-Machine Era: A forecast of new and emerging language technologies*. University of Jyväskylä. <https://doi.org/10.17011/jyx/reports/20210518/1>
32. Shuy, R.W. 1993. *Language crimes: The use and abuse of language evidence in the courtroom*. Cambridge, MA: Blackwell.
33. Singh, A., N. Singh, S.K. Singh, and S.K. Nayak. 2023. Cyber-crime and digital forensics: Challenges resolution. In *2023 International conference on computer communication and informatics (ICCCI)*, 1–7. <https://doi.org/10.1109/ICCCI56745.2023.10128333>.
34. Sousa-Silva, R. 2013. *Detecting plagiarism in the forensic linguistics turn* [Unpublished PhD Thesis]. Birmingham: Aston University.
35. Sousa-Silva, R. 2014. Detecting translingual plagiarism and the backlash against translation plagiarists. *Language and Law / Linguagem e Direito*, 1(1), 70–94.
36. Sousa-Silva, R. 2021. Plagiarism: Evidence-based plagiarism detection in forensic contexts. In *The Routledge handbook of forensic linguistics*, 2nd ed., ed. M. Coulthard, A. May, and R. Sousa-Silva, 364–381. New York/London: Routledge.
37. Sousa-Silva, R. 2022. Fighting the Fake: A Forensic Linguistic Analysis to Fake News Detection. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*. <https://doi.org/10.1007/s11196-022-09901-w>
38. Sousa-Silva, R. 2023. Forensic Linguistics: The potential of language for law enforcement in the digital age. *European Law Enforcement Research Bulletin, Special Conference Edition*, 23–32.
39. Trudgill, P. 1974. *The social differentiation of English in Norwich*. Cambridge: Cambridge University Press.
40. Wall, D.S. 2001. Cybercrimes and the Internet. In *Crime and the Internet*, 1–17. Abingdon: Routledge.
41. Wall, D.S. 2021. The transnational cybercrime extortion landscape and the pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. *European law enforcement research bulletin, special conference edition* (5).
42. Weigand, E. 2008. Towards a common European legal thinking: A dialogic challenge. In *Paradoxes of European legal integration*, ed. A.L. Kjær, H. Petersen, and M.R. Madsen. London: Routledge.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## Authors and Affiliations

**Rui Sousa-Silva**<sup>1,2</sup> 

✉ Rui Sousa-Silva  
rssilva@letras.up.pt

<sup>1</sup> Faculty of Arts and Humanities, University of Porto, Via Panorâmica, S/N, 4150-564 Porto, Portugal

<sup>2</sup> CLUP - Centre for Linguistics, University of Porto, Porto, Portugal