Legal and Regulatory Structure Prevailing in the UK related to Data Privacy and Public Surveillance

Amarachukwu Grace Nwosu

School of Architecture, Computing and Engineering Department, University of East London

Received: 05 August 2024/ Revised: 10 August 2024/ Accepted: 16 August 2024/ Published: 31-08-2024
Copyright @ 2024 International Journal of Engineering Research and Science
This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (https://creativecommons.org/licenses/by-nc/4.0) which permits unrestricted Non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract— *Over the years, the Internet has changed from a system essentially concerned with providing data, to a channel for communication and social cohesion (Fuchs et al.,2013). Criminals go fastidious to hide illegal activities, which is why surveillance is essential for the purpose of investigation. By carrying out surveillance, detectives can discover proof required to substantiate legal suit, or imprison a lawbreaker. This paper uses the IRAC method to explain the prevailing legal and regulatory structures in the EU and UK with respect to social media surveillance. It also gives an in-depth analysis of the rights of a person or citizen to social media privacy. It outlines the dangers of social media surveillance by authorities, and demonstrate different case laws and rulings regarding violations of citizens' right of privacy by different authorities.*

Keywords— Social media surveillance, privacy rights, EU data protection, UK data protection, IRAC method, legal and regulatory framework, surveillance and crime, digital rights.

I. INTRODUCTION

Surveillance can be used by detectives to track a person's movements, in search of activities that may implicate or vindicate them of skepticism. It can facilitate in identifying delinquent groups, as well as the connection between a suspected person, and their allies. It can ultimately provide helpful insights into the formation and strategies of criminal groups. There are basically six types of surveillance, and they include: electronic surveillance, physical surveillance, computer surveillance, social media surveillance, financial surveillance, and biometric surveillance.

Creation of social applications such as the X, TikTok, Facebook, was endorsed by Web 2.0, and it laid the foundation for Web 3.0, the succeeding initiation of the web which tackles glitches in a different way using same technologies (Will Kenton, 2023). It supports users to bring contents rather than merely watching it. With the arrival of these social applications, comes enormous supply and storage of individual data, which can in turn be methodically assessed, sold, or used for targeting users. The regulation of social media is a difficult and demanding issue as it comes with certain number of challenges like, (i) Outlining harmful content; establishing what forms a harmful content is complicated, as there is no distinct agreement on what content should be regulated, or permissible to stay on social media platforms. (ii) Implementing Regulations: enforcing regulations on social media platforms can be tough, because these platforms are situated in countries with diverse legal systems, and getting assistance from oversea governments can be challenging. (iii) Counterpoising uninhibited speech: striking a balance between the need to defend free speech, and the need to protect users from harmful content can be delicate while trying to regulate social media.

The degree of violation caused by social media surveillance by the government is overwhelming. There are reports of misuse even in countries with significant protections for basic freedoms. For instance, in the UK, London police seemingly monitored almost 9,000 advocates around the diplomatic field, using analysis based on emotions on information scratched from Facebook, X, and other social media platforms. Several of these advocates had no illegal background. Furthermore, there is a disturbing rise in the number of countries where social media users have been detained for their genuine online activities (Shahbaz & Funk, n.d).

II. FACTS OF THE MATTER (ISSUES)

Authorities are progressively procuring state-of-the-art technologies to check the activities of their citizens on social media. Social media surveillance is the gathering, and managing of private information extracted from digital interaction platform, through mechanized skills, that permits evaluation of huge amounts of content, organization, and metadata. It cannot be discharged as not so much intrusive. Large number of people all over the world use this platform to connect with friends and loved ones. They also use it to voice their social, religious, and political views. China spearheads the generating, use, and distribution of social media surveillance devices (Shahbaz & Funk, n.d). As people continue to share pictures, videos, and posts, social media continues to grow.

Social media can put a person's personal information at risk without their knowledge, which is why information privacy is crucial as users set off digital tracks every day. For example, in July 2022, twitter was breached, and over 200 million users had their email addresses published on the dark web. These published emails can provide criminals with the information they require to carry out mischievous acts. A second example is, European Data Protection Board, fining Meta 1.3 billion dollars sometime in May 2023, because they violated European Union privacy laws by collecting, and transferring individual information of European Facebook users to United states servers. The consternation for privacy is at the foreground as cyberattack is in the news on a daily basis (Hetler, 2024). The concern for information privacy, triggered Federal Agencies, and U.S. states towards end of 2022, to prohibit workers from using TikTok on devices owned by government. They believe that since TikTok is owned by a Chinese company, they may likely use the app to acquire classified information about their government through these devices.

Majority of the information shared by users on social media platform through profile information and posts are done willingly. However, information can equally be unintentionally delivered through tracking cookies. These cookies trace the online activities of users, their acquisition record, and their webpage assessments. The information is afterwards collected and organized in sections, which in turn, is sold by information brokers for marketing intentions. Such sections may include: parents, fitness fanatics, animal lovers. Now with these sections, it is easy for organizations to modify advertising campaigns to social media users. In 2023, the information from Federal Trade Commission shows that people revealed losing over 10 billion dollars to scam, making it the largest scam losses so far recorded (Tressler, 2024). Scammers and promoters can still acquire the following information from a user on social media even when their account is private: location information, status updates, shared contents, employment details, personal interests, and religious beliefs.

Officials and scammers can obtain sufficient data to spy on user, or steal identities with the enormous amount of information on social media accounts. Certain ambiguities in privacy controls can place a user's data in jeopardy when using social media. Some social media privacy issues include:

- **Incorrect data:** Some individuals can disseminate misleading information on social media, while some trolls will seek to manipulate users' reactions by inciting them into intense arguments. It is therefore imperative to verify information from social media before utilizing it.
- **Privacy setting flaws:** Most private accounts on social media may not be as clandestine as users assume. For instance, a user may share information with a group of friends, once that information is reposted by those friends, it ends up before an entirely different audience.
- **Information exploitation:** Both cyberthieves and officials can begin spying on a target from information openly posted on social media. Cyberthieves can collect data such as email addresses, phone numbers, usernames, to plan phishing scams on users.
- **Setting of location:** A user's individual data, coupled with their location, is able to provide correct information to their profile. If a person turns off their location settings, the location app settings can still trace the person's location, because there are ways to aim their devices through phone turrets, websites, and public wi-fi.
- **Cyberbullying and harassment:** some mischievous persons can dox a person just for the intent of causing them harm.
- **Risk of viruses and malware:** When criminals hijack social media accounts, they use it to distribute malware to the contacts of the hijacked accounts. This can infect users with adverts, slow down their computers, and also steal delicate data.

Sometime in May 2013, Edward Snowden, a 29-year-old former technical assistant for the CIA, disclosed the worldwide surveillance activities of large parts of the web, most especially the social networks, organized by the National Security Agency. This action, has thus, raised privacy concerns on the internet. Do social media users actually care about their online privacy?

Do they believe that their online information is secure? Are users truthful about the information they post? The answer to these questions could be obtained by analyzing the empirical study conducted by Knautz and Baran (2016), between 22 July and 11 August 2014, on 304 people categorized by age, sex, and academic background, using an online questionnaire. The people who participated in the study, were queried about their conduct on social media, as well as their individual view about online privacy. The study shows a strong connection between the extent of people's divulgence on social media and age. The academic background of a person does not appear to influence their behavior in respect to their social media divulgence. However, the knowledge of the harms associated with abuse of privacy, has small connection with a person's maturity and education (Knautz & Baran, 2016). Regulating the kind of data shared to groups remains one of the most conventional ways of protecting a person's online privacy. Social media users know about the dangers of privacy violation, but appear willing to disregard them, especially when evaluated against the profit they get from using it.

Big Brother Watch, the UK civil rights group has made public, a key document about the UK government's social media surveillance. The 106-page article titled 'Ministry of Truth', reconnoiters at least five sinister divisions inside the UK government: the 77th Brigade, the Government Information Cell, the Intelligence and Communications Unit, the Rapid Response Unit, and the Counter Disinformation Unit. Each of these divisions, prevailingly use social media to collect data about people (Moody, 2023). The article specifies the behaviors of these divisions, and also proves that their evidence is gotten by means of liberty of data demand. According to the information made available to Big Brother Watch, by a whistleblower, about the comment made by the 77th brigade: "home observation of citizens online appeared not to be determined by a wish to tackle the fears and interests of the public, rather to discover forces for conformity with debatable government policies", typically explains the damage social media surveillance activities brings to privacy (Moody, 2023).

"The dangers that surveillance causes to privacy and equality are often spoken in the abstract, practical expressions, or as imminent dangers". Though, the effect of disproportionate surveillance in the UK is being experienced now, just that oftentimes, the opinions of those impacted the most are not heard (Hurfurt, 2023). Some of the issues of social media surveillance includes:

- **Destroys right:** Social media surveillance gradually destroys a person's right; fairness entails exciting open space devoid of continuous surveillance.
- **Infringes privacy:** Officials can save and study personal details of individuals like, their religious beliefs, sexual inclination, individual relationships through surveillance, and disclose them to authorities.
- **Impends immigrants' rights:** Individuals can be denied entry by immigration officers on the basis of their religious, political, and social views conveyed on their social media platforms.
- **Allows discrimination:** Analytical and human predisposition can enable untrue and dangerous ideas, hence, inexplicably affecting relegated groups.
- **Limits uninhibited expression:** Social media surveillance can cause individuals to desist from frankly making known their positions on political, religious, and social issues, for fear that their communication could be documented by officials, and possibly used against them.
- **Restrains right of association:** Surveillance of social media by authorities can make individuals more unlikely to join certain parties or groups.
- **Challenges integrity:** Social media surveillance disavows independent legal standards of "justified suspicion", and "good reason", and handles everybody as a crime suspect.

III. RELEVANT ACT, DIRECTIVES (RULES)

As technology improvements have made monitoring actions simpler, surveillance laws in the UK have also become even more significant currently. It is essential to know what the laws say about surveillance in the UK and EU, amidst the use of surveillance cameras, CCTV systems, and other methods of monitoring. Some of the laws governing surveillance in the UK include: Investigatory Powers Act 2016 (IPA), Data Protection Act 2018 (DPA), Human Rights Act 1998 (HRA), General Data Protection Regulation (GDPR) as amended, Regulation of Investigatory Powers Act 2000 (RIPA), alongside the published codes of practice from the Home Office, Investigatory Powers Commissioner's Office (IPCO), previously the Office of Surveillance Commissioners (OSC), and the Information Commissioner's Office. The Privacy and Electronic Communications Regulations (the PECR) 2003 (EC Directive), execute the prerequisites of Directive 2002/58/EC, (the "ePrivacy Directive" as amended by Directive 2009/136/EC), which specifies a precise number of privacy rules to integrate the management of individual information by the telecommunications section. The essence of these policies is to explain how the Authorities may use social media when performing investigations, or carrying out other duties. This includes scrutinization of child protection, examination of trading paradigms, preemptive assessments in comparison to profits and incomes, and violations of the

Authorities' guideline. It ensures that any surveillance, investigation, or data collection requiring the use of social media is performed properly and lawfully in conformity with a person's human right. Social media, otherwise known as Social Networking Service (SNS), is a web-based resource which permits individuals, or businesses to create a public profile. Few of its characteristics include: the capacity to display a list of other people whom a user has association with, capacity to permit posting of photos and videos which can be viewed by many, and the capacity to surf and see list of associations made by other people in the platform.

The Center for Democracy & Technology (CDT), identifies an interconnected threat to privacy, resulting from individual data on social media posts. This moves beyond just data extraction of shared posts; it is an outcome of current attempts to permit researchers to have understanding of social media dynamics, by providing them authorized access to huge data. Example is the Article 40 of the EU's Digital Services Act (DSA), which requires organizations that are labelled as big online platforms, to provide appropriately evaluated researchers access to information, though hinged on some specific conditions. One of the confusing issues in this matter according to CDT report, is that while the Digital Service Act took effect in November 2022, a lot of facts are still indistinct. These will be fixed using "delegated acts"; extra stipulations released by the European Commission. The way to resolve the new right to access social media with the European Union's supreme GDPR (General Data Protection Regulation), is one of the paramount concerns at the moment. This simply shows that many social media posts include individual data that is subject to the GDPR.

RIPA was passed to determine ways by which the authorities may interfere with privacy rights in agreement with the law, and also in order to integrate the stipulations of Article 8(2) in English law. The aim is to shield the administrators and Commission in an investigation. The structure of RIPA is to affirm that an approval for covert surveillance, shall be legally recognized for every purpose, but that such legal recognition, could be approved, only if the officer is convinced that what is intended, is required and fair. If the approval methods presented by RIPA are adhered to, they offer shield to local authorities, and also to officials, with regards to difficulties associated with acceptability of evidence, applications under the Human Rights Act 1998, and objections to the Investigatory Powers Tribunal. The Act is backed by latest statutory Codes of Practice issued in 2018. They are the 'Covert Surveillance and Property Interference' and the 'Covert Human Intelligence Sources' (CHIS) Code of Practice. RIPA demands the local authorities to respect the stipulations of the Codes, which are admissible in any court as proof in criminal and civil actions. Although, the modifications which was operational on 1st November 2012, imply that a district authority may only approve directed surveillance under RIPA, to identify or avert illegal crimes punishable by full term of 6 months incarceration, whether on accusation or sentence. District authorities cannot approve directed surveillance for the aim of stopping chaos, except when it concerns unlawful crime punishable by a full 6 months incarceration term.

In May 2001, Investigatory Powers Commissioner's Office; an Inspectorate, was created in the Office of Surveillance Commissioners (OSC), to retain the evaluation of the practice and implementation of the powers, and responsibilities enforced by RIPA. In October 2017, this Office was substituted, and is presently called the IPCO (Investigatory Powers Commissioner's Office), and is controlled by the Investigatory Powers Commissioner. In August 2018, the latest Procedures and Guidance record, was released by the Investigatory Powers Commissioner, and is accessible on the Council's network. Authorities generally are obligated by RIPA to release all such records to the Investigatory Powers Commissioner, to enable him perform his tasks. Duly, the local authorities' custom and procedure is to conform entirely, and also conciliate between defending a person's basic privacy right, and carrying out a covert surveillance. One may ask, what is meant by covert surveillance? In accordance with RIPA section 48(1), surveillance is covert, only if it is executed in a way that is intended to ensure that the individuals who are being surveilled are unaware that they are under surveillance. Act 2000 outline, does not apply if surveillance is exposed to a person under examination. Furthermore, when surveillance is covert but not invasive, it is said to be 'directed'. Directed surveillance is any prearranged surveillance movement, embarked covertly, for the aim of a precise scrutinization, in a manner that is apt to end in getting a person's private data.

Whereas an individual may have a minimal expectation of privacy on social media, covert surveillance of the person's public activities can still result in getting their personal data. This is most likely the situation where the individual has a logical presupposition of privacy though acting in public. In an event where covert surveillance is executed under 'immediate response', in a manner that it is satisfactorily impracticable to get approval, it will not require a directed surveillance approval according to the Covert Surveillance and Property Interference Code of Practice of the 2000 Act. For example, a policeman who just stumbled on a suspect while on guard, would not need an approval to hide himself and surveil the individual. While using social media for research and investigations, officials should be careful not to drift into surveillance. They should not assume that because social media is an open space, it exempts the need for an approval before surveillance can take place. The use of social media in situations that require logical expectation of privacy, requires approval especially when the surveillance

will take longer that one week. Furthermore, certain actions like opening a fake or unknown account, and entering locked groups with the intention of investigation is also most likely to need an approval, except the official's identity is disclosed from the beginning.

The Human Rights Act 1998 regulates surveillance in the UK, it integrates the European Convention on Human Rights (ECHR) into UK law, together with right to privacy. This implies that local authorities should make sure that any surveillance they perform is essential and fair, and does not unjustifiably breach the rights of a person. Regulation (European Union) 2016/679; GDPR (General Data Protection Regulation), was the primary data protection legislation in the United Kingdom prior to their exit from the Eu on the 31st December, 2020. The GDPR voided the Data Protection Directive 95/46/EC, and this resulted in better compliance with the data protection law throughout the European Union member states. Certain conditions in the GDPR, can be modified in the national laws of the European Union member states. Hence, the Government of the United Kingdom issued the Data Protection Act 2018(DPA 2018), and a number of successive modifications that encompasses those sections of the GDPR which are not included in the Eu law, but could be added by the European Union member states. The Data Protection Act 2018 became operational on 25th May, 2018. The Investigatory Powers Act 2016 (IPA) is correspondingly another important UK law on surveillance, that strengthens and revises the prerogatives of local authorities to perform surveillance. However, IPA demands that local authorities must get approval through the secretary of state or a Judge before conducting surveillance.

Protection of information is a basic right in the European Union (Article 8 of the Charter of Fundamental Rights). It is matched by various other mediums like, the Data Protection Regulation (EU) 2018/1725, which sets off the information protection constraints with respect to managing of individual information by the EU organizations and agencies, relevant to the European Research Executive Agency (REA). People whose individual information is managed by REA, could apply some rights set up in Articles 14-24 of Regulation 2018/1725. In some cases, REA can constrain a person's information right, in conformance to the rules of Article 25 of the Regulation, centered on its evaluation of the Steering Committee, on internal rules regarding constrain of certain rights of a person's information. A person can be notified of their rights through DPN (Data Protection Notices), communicated by the data controllers and the DPR (Data Protection Records), accessible in the Central Public Register of Records. Directive (EU) 2016/680, defends a resident's basic right to information protection, anytime delicate information is being used by law enforcement government department, for the intent of prosecution. It ensures that the individual information of accused persons, witnesses, and targets are protected accordingly as well as aid international cooperation, in the battle against criminality and violence.

Directive (EU) 2016/680 became operative on 5 May, 2016 and was transferred into EU countries' national law on 6 May, 2018. Countries in EU have raised national bodies in charge of protecting individual's information in agreement with Article 8(3) of the Charter of Fundamental Rights of the EU. The GDPR regulation purposes to restructure collaboration between Data Protection Authorities when implementing the GDPR in international cases. The EDPB (European Data Protection Board), is a self-regulating body, that ensures the coherent implementation of information protection rules in every part of the European Union. EDPB is instituted by the GDPR, and is comprised of the spokespersons of the national data protection authorities of the EU/EEA (European Economic Area), and the directors of the European Data Protection. The basic tasks of the EDPB include: directing the European Commission on subjects connected to the protection of individual data, and any fresh recommended legislation in the EU, offering help on basic models of the Law Enforcement Directive and the GDPR, and finally approving mandatory resolutions in disagreements between the national managerial authorities. A Data Protection Officer, as selected by The European Commission is in charge of monitoring and implementation of information protection rules in the European Commission. The officer objectively ensures the domestic implementation of information protection rules in collaboration with the European data protection directors.

The European ePrivacy Regulation is a crucial amendment to the current ePrivacy directive of 2002, and it is the "lex specialis" to the GDPR. Lex specialis means "law governing a specific matter". The legal doctrine "lex specialis derogat legi generali" (a special law overrides laws that govern general matter), is welcomed by the European Union. According to Article 1, Subject matter, the regulation draws up rules concerning the protection of basic rights and freedom of an individual, with regards to the use of electronic interaction service in managing personal data. It also draws up the rules regarding the protection of the basic rights of the authority, in the use of electronic interaction services, especially their rights to acceptance of interactions. EU member states, in February 10 2021, settled on a bargaining order for amended rules on the protection of privacy and discretion, in the use of electronic interaction services. The amended ePrivacy rules, outline the circumstances in which internet access providers are permitted to process or access information saved on consumer's machines. The rules also include information conveyed on networked devices, to ensure complete protection of privacy rights and to encourage a reliable IoT

(Internet of Things). The rules apply when consumers are in the European Union, and also include situations where the processing or the service provider is situated outside the European Union. Therefore, as a principal rule, any information through electronic interaction is private, so any form of interference, monitoring or processing of such information by anybody apart from the consumer is illegal, except when approved by the ePrivacy regulation.

IV. ANALYSIS OF RELEVANT CASE LAWS

The assimilation of Article 8 into the UK law through the Human Rights Act 1998 simply implies that a public or government agency involved in any interference practice with a person's privacy should be able to prove that the said surveillance is: required, lawful, commensurate to the intention, and performed in agreement with one of the legal objectives laid out in Article 8(2) of the ECHR. In the case of Prismall v. Google UK Limited and Deepmind Technologies Limited [2023] EWHC 1169 (KB); about the alleged abuse of medical reports of 1.6 million patients. The reports were moved to DeepMind, a subdivision of Google focusing on artificial intelligence research and development. The aim of moving the reports was to help in creating an app intended to assist health care specialists to discover and treat people with severe kidney damage. The plaintiff, Andrew Prismall was one of the patients impacted. He argued that moving the reports without the consent of the patients was an abuse of private information, and requested for costs over loss of control of his personal data, and that of the other impacted patients. Although the court acknowledged Prismall's worries, it dismissed the claim, establishing the fact that there was no reasonable outlook of proving a logical expectation of privacy among the patients. It also states that the diverse nature of the patients' conditions disallows pursuing an action.

In the survey by the International Association of Chiefs of Police (IACP), "2011 IACP (2011, p.3 as cited in Brunty & Helenek, 2012), 88.1% of law officers use social media among the 800 law officers surveyed. Greater part of them stated that social media has assisted them in solving crime. From the investigation conducted by Privacy Internation, David Feldman, who is Rouse Ball English law professor from the university of Cambridge, disputed that before the passing of the Human Rights Act 1998 (HRA), there was no recognized right to privacy in UK law. Though people could petition to the European Court of Human Rights, if they suffered any violation of their right to privacy under the Article 8 of the ECHR (European Convention on Human Rights). Following the passing of the Human Rights Act, the ECHR turned out to be part of an established home law, and also an over-all right to respect for family and private life under Article 8 in the UK. As a result, it became illegal for any public agency to act in a way that intrudes a person's privacy, except the public agency can indicate any particular exceptions enclosed in Article 8.

Also, In the case of a popular model Naomi Campbell and Mirror Group Newspaper [2004] UKHL 22; Mirror Group Newspaper published an article about her drug addiction, and successively backed it up with some photographs of the model exiting a gathering for drug addicts. The model requested costs for violation of privacy relative to the covertly taken photographs. However, she acknowledged that the newspaper was permitted to publish the evidences of her addiction and treatment, following her earlier public statement. She won the trial where it was held that the information objected was private, and publication was not in the interest of the public. The court of appeal however, agreed that the respondent's petition, on the ground that the extra information of the model's medical treatment, was required to prove the integrity of the story, and in the interest of the public. Campbell however appealed to House of Lords. The House of Lords maintained that the appropriate experiment to establish if information was private, was to consider whether a random sensible individual, subjected in the exact situation as the Model, would find the exposure of the information invasive. The Court stated that guarantee of privacy, was a necessary part of Campbell's treatment therapy in relation to her physical and mental health, and that details of her therapy, consequently formed private information which resulted in privacy obligation. The press exceeded their editorial boundary. Meanwhile, regarding the photographs taken outside the gathering, the Court acknowledged that a person may have a logical privacy expectation in public, and that this expectation was unreasonably violated in this case.

The establishment of HRA has assisted in making sure that the privacy of the people is well secured. However, right to privacy alone is incapable of providing enough base for the protection of people against intrusive surveillance, or processing of information. For example, in the landmark judgement in relation to UK's mass surveillance, European Court of Human Rights (ECtHR) ruled that the UK's mass surveillance, violated the people's right to privacy. The mass surveillance was revealed by Edward Snowden. UK's negligence to use protections of identity, location, and address violated the people's right to privacy under Article 8 ECHR. Though the ruling involved the Regulation of Investigatory Powers Act 2000 (RIPA), which has been significantly overtaken by the Investigatory Powers Act 2016 (IPA), much of the court's reflections relate to the new law. The UK's surveillance system subject to RIPA was unsolicited, simply implying that the UK people's individual information was collected indiscriminately, without any hint of suspicion, or proof of crime, and the system was indefinitely operative.

Furthermore, in the case of Bekoe v. Islington LBC [2023] EWHC 1668 (KB), concerning the abuse of private information by a local authority. Islington LBC, a local authority abused the private information and confidential details of Bekoe's finances, by retrieving and distributing them during legal trials, thereby breaching the GDPR. Bekoe stated that his information was gotten illegally, and claimed that Islington had breached the GDPR by abusing a Data Subject Access Request (DSAR), which he tendered. He stated that Islington was responsible for loss of legal documents following an unfinished confession, a four-year delay, and negligence in providing sufficient protection over personal data. The court resolved that Islington had failed to show that the misuse of Bekoe's private information was commensurate to the intention. The expectation of privacy, outweighs other interests, consequently violating Bekoe's GDPR rights. The court awarded him 6,000 pounds in costs.

Also, in the case of ZXC v Bloomberg [2022] UKSC 5; a pivotal privacy case resolved by the UK Supreme Court. It was contemplated whether an individual under criminal investigation, prior to being arraigned, has a logical hope of privacy, about information concerning the investigation. ZXC is a regional CEO of a Plc overseas, and in charge of operations. An Editorial was published regarding the Plc's operations for which ZXC was liable. The Editorial was centered on subjects of a letter sent to a foreign law enforcement agency, by a law enforcement agency in the UK, investigating the activities of the Plc within the district. ZXC demanded a logical hope of privacy, based on the details of the criminal investigations into his activities, revealed through the letter. He also claimed that the publication of the editorial by Bloomberg resulted in violation of that confidential information. There were three subjects before the court:

A) If the Court of Appeal was mistaken to maintain that there is a common rule, relevant in the current lawsuit, that an individual under criminal investigation has, prior to being arraigned, a logical hope of privacy regarding information relating to that investigation.

B) If the Court of Appeal was mistaken to maintain that, in a lawsuit where a claim for violation of confidence was not followed, for the fact that the information printed by Bloomberg about the investigation, came from the confidential records of the law enforcement, made the information private thereby weakening Bloomberg's power to bank on the public interest in exposing it.

C) If the Court of Appeal was mistaken to maintain the findings of one Nicklin J, that the plaintiff had a logical hope of privacy with respect to the printed information complained of, and that Article 8 and 10 correspondingly went down in support of the plaintiff.

The Appeal was dismissed by the court on all three bases, hence, the practice is established that there is, as a lawful basis, a supposition that there is a logical hope of privacy relative to facts of a criminal investigation prior to arraignment.

V. CONCLUSION

The use of social media surveillance for investigative purposes is more consistent across forces than it is for communication purposes. A study of the internal policy documents, by Egawhary (2019), of UK Law Enforcement Agencies' use of social media in surveillance, finds that they deliberate five surveillance aspects of social media: common surveillance of the residents, inciting residents to surveil each other, supervisory surveillance, homologous surveillance and surveillance with the intention of investigation. Several of the cases involving surveillance begins with a concern of the actions' agreement with Article 8(2) in accordance with the requirements of the law. For example, the Article states that, "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

In my analysis however, I observed that Article 8(2) has failed in attaining sufficient amount of clarity regarding the limit which surveillance methods can be used, and this has intensified the danger of using surveillance in an illogical manner.

I recommend that in a situation whereby Article 8(2) cannot be amended to provide more clarity, then, in addition to whatever training is being given to public authorities entrusted with implementing Article 8(2), they should be made to understand in clear terms, the importance of moral and integrity, in ensuring that the implementation of the Article is free, fair, credible, in good fate and without bias.

REFERENCES

[1] Fuchs, C, Boersma, K, Albrechtslund, A & Sandoval, M (2013). Internet and Surveillance: The Challenges of Web 2.0 and Social Media. Routledge. New York.

[2] The Washington Post & O' Harrow, Jr (2014, Jan 9). Zero day: the threat in cyberspace. Diversion books. (kindle edition).

[3] Shahbaz, A., & Funk, A. (n.d). Social Media Surveillance, Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance Freedom House. https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance

[4] Brunty, J & Helenek, K (2012). Social Media Investigation for Law Enforcement. Taylor &Francis group.

[5] Types of Surveillance for Investigations Explained. (April 25, 2023). NITA. https://investigativeacademy.com/6-types-of-surveillance-for-investigations-explained/#:~:text=Surveillance%20takes%20many%20forms%2C%20including,threats%2C%20and%20investigate%20criminal%20activity

[6] Will, K (2023, July 30). What is Web 2.0? Definition, Impact, and Examples. Investopedia. https://www.investopedia.com/terms/w/web.20.asp#:~:text=Web%202.0%20describes%20the%20current,aftermath%20of%20the%20dotcom%20bubble.

[7] Jake Hurfurt (2023). State of Surveillance in 2023. Big Brother Watch. https://bigbrotherwatch.org.uk/wp-content/uploads/2023/12/State-of-Surveillance-Report-23.pdf

[8] Home Office Covert Surveillance and Property interference, August 2018. (2020, May 24). PI. https://privacyinternational.org/long-read/3532/home-office-covert-surveillance-and-property-interference-august-2018

[9] Moody, G (2023, February 1). UK Government Is Engaged in Large-Scale Surveillance of Social Media. Private Internet Access. https://www.privateinternetaccess.com/blog/uk-social-media-surveillance/

[10] Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st Century: Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization. Criminal Justice Review, 36(3), 253-268. https://doi.org/10.1177/0734016811399421

[11] What Laws Are There on Surveillance in the UK? (2023, March 24). Able Investigations and Enforcement Services. https://ableinvestigations.com/what-laws-are-there-on-surveillance-in-the-uk/#:~:text=Under%20the%20IPA%20and%20RIPA,rights%20of%20individuals%20are%20protected

[12] Regulation of Investigatory Powers Act 2000 https://proceduresonline.com/trixcms2/media/8508/ripa-2000-using-social-media-as-a-surveillance-tool.pdf

[13] History of the UK Regulator's concerns regarding Local Authority use of social media monitoring. (2020, May 24). PI. https://privacyinternational.org/long-read/3531/history-uk-regulators-concerns-regarding-local-authority-use-social-media-monitoring

[14] Kouvakas, L (2023, August 22). Changes to UK Surveillance Regime May Violate International Law. Just Security. https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/

[15] Methodology: Social Media Monitoring by Local Authorities. (2020, May 24). PI. https://privacyinternational.org/report/3530/methodology-social-media-monitoring-local-authorities

[16] Surveillance: Citizens and the State- Constitution. (2009). https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm

[17] Teacher, Law. (November 2013). Campbell v Mirror Group Newspapers - 2004. Retrieved from https://www.lawteacher.net/cases/campbell-v-mirror-group.php?vref=1

[18] The use of social media monitoring by local authorities- who is a target? (2020, May 24). PI. https://privacyinternational.org/explainer/3587/use-social-media-monitoring-local-authorities-who-target

[19] Use of social media in investigations policy and procedure 2020-21. (n.d). https://www.colchester.gov.uk/info/cbc-article/?catid=policy-framework-local-choice&id=KA-01480

[20] Egawhary, E.M (n.d). Surveillance and Society: The surveillance Dimensions of the Use of Social Media by UK Police Force. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12916/8481

[21] When Local Authorities aren't your Friends. (2020, May 24). PI. https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends

[22] Article 8: Respect for your private and family life. (2021, June 24). Equality and Human Rights Commission. https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life#:~:text=and%20family%20life-,Article%208%20protects%20your%20right%20to%20respect%20for%20your%20private,and%20emails%2C%20for%20example

[23] Head of Law and Governance Stratford-on-Avon District Council. (2020, December). Use of Social Media in Investigations Procedure. https://www.stratford.gov.uk/doc/210080/name/SDC%20Use%20of%20Social%20Media%20in%20Investigations%20Procedure%20Version2%20.pdf

[24] The Regulation of Investigatory Powers Act (RIPA) Policy and Procedure. (2020, November 25). Lancaster City Council. https://committeeadmin.lancaster.gov.uk/documents/s82166/RIPA%20and%20Social%20Media%20Policy%20v3%201.1.pdf

[25] REA privacy policy and social media use. (n.d). European Commission. https://rea.ec.europa.eu/rea-privacy-policy-and-social-media-use_en

[26] Hetler, A (2024, April 23). 6 common social media issues. TechTarget. https://www.techtarget.com/whatis/feature/6-common-social-media-privacy-issues

[27] Clarke, L (2024, January 3). Britain's got some of Europe's toughest surveillance laws, Now it wants more. Politico. https://www.politico.eu/article/uk-bulking-up-spying-regime-breakneck-speed/

[28] Data protection in the EU. (n.d). European Commission. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

[29] The European ePrivacy Regulation. (2021, February 10). https://www.european-eprivacy-regulation.com/

[30] Overview- Data Protection and the EU. (n.d). ICO. https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#:~:text=in%20the%20EEA.-,Does%20the%20GDPR%20still%20apply%3F,Act%202018%20(DPA%202018)

[31] Sachowski, J (2016). Ensure Legal Reviews. In J. Sachowski (Eds.), Implementing Digital Forensic Readiness. (pp. 143-149). Syngress. https://www.sciencedirect.com/science/article/pii/B9780128044544000149

[32] Osborne, M (2006). Information Security Laws and Regulations. In M. Osborne (Eds.), How to Cheat at Managing Information Security/ (pp. 71-86). Syngress. https://www.sciencedirect.com/science/article/pii/B9781597491105500117

[33] Zorzetto, S (2012, September 3). The Lex Specialis Principle and its Uses in Legal Argumentation. An Analytical Inquire.

[34] The final text of the Digital Services Act (DSA). (2022, October 19). Cyber Risk GmbH. https://www.eu-digital-services-act.com/Digital_Services_Act_Article_40.html

[35] UK: Europe's top court rules UK mass surveillance regime violated human rights. (2021, My 25). Amnesty International. https://www.amnesty.org/en/latest/press-release/2021/05/uk-surveillance-gchq-ecthr-ruling/

[36] UK: Stop social media monitoring by local authorities. (2020, June 10). EDRi. https://edri.org/our-work/uk-stop-social-media-monitoring-by-local-authorities/

[37] Nakutavičiūtė, J (2024, January 01), What are the most common social media privacy issues?. NordVPN. https://nordvpn.com/blog/social-media-privacy-issues/

[38] Hickman, T & Devine, J (2023, July 20). Data Protection Laws and Regulations UK 2023-2024. https://iclg.com/practice-areas/data-protection-laws-and-regulations/united-kingdom

[39] The Human Rights Act Is A Vital Defense Against Surveillance. (2018, November 8). https://eachother.org.uk/the-human-rights-act-is-a-vital-defence-against-surveillance/

[40] Jeanis, Michelle & Muniz, Caitlyn & Molbert, Courtney. (2019). Law Enforcement and Social Media Usage: An Analysis of Engagement. Policing: A Journal of Policy and Practice. 15. 10.1093/police/paz026.

[41] Todd, E, Andrews, J.J & Lysik, A (2024, February 20). 2023 UK Data Protection and Privacy Case Law Update. ReedSmith. https://www.reedsmith.com/en/perspectives/2024/02/2023-data-protection-and-privacy-case-law-overview

[42] Lipschultz, J.H (2023). Social Media Communication: Concepts, Practices, Data, Law and Ethics. Routledge. (Fourth edition).

[43] Top 10 Privacy and Data Protection Cases 2022. (2023, January 1). T he Privacy Perspective. https://theprivacyperspective.com/2023/01/01/top-10-privacy-and-data-protection-cases-2022/

[44] European Convention on Human Rights- Article 8 (nd). FRA. https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0

[45] Egawhary, E.M (2019). Surveillance & Society. The Surveillance Dimensions of the Use of Social Media by UK Police Forces. https://eu.docs.wps.com/l/sIHW88LHlAb7vwrIG?v=v2.