



RULING (0105 K104-10)

The investigation has been closed since the crime of unlawful intelligence activities could not be substantiated, crimes against the Personal Data Act cannot be investigated and there are no grounds to suspect that breach of professional confidentiality was committed.

Grounds for the ruling

Introduction

At the beginning of November 2010, Norwegian media related that US authorities had been monitoring individuals in several countries since the year 2000 as a part of their security measures to protect US embassies and US embassy staff. There was information to indicate that the US Embassy made use of separate premises in downtown Oslo, where 15-20 former police officers made up a “Surveillance Detection Unit” (SDU) which monitored and photographed a large number of people, for example, during demonstrations. The information was reportedly entered into a database named “Security Incident Management and Analysis System” (SIMAS). On the website for the US Ministry for Foreign Affairs, one could also read that this register could contain biometric data such as hair colour, race, height and skin colour.

After the Swedish Security Service and the US Embassy in Stockholm met on 5 November, a press release from the Swedish Security Service confirmed that the Embassy was performing surveillance of a nature similar to that in Norway.

Based on this information, I decided to initiate an investigation on suspicion of unlawful intelligence activities. During the investigation, as is usual procedure, a consideration was also made of criminal offences other than that which gave rise to the investigation. Consequently, the investigation also considered whether crimes against the Personal Data Act and breach of professional confidentiality could also have been committed.

Legal background

Illegal intelligence activities

The regulation concerning *illegal intelligence activities* in Chapter 19, Section 10 of the Penal Code covers two separate types of illegal intelligence gathering. The offence that this investigation focuses on is detailed in the second paragraph of the clause, which states that:

A person who, with the intent of aiding a foreign power, secretly or by fraudulent means conducts in the Realm activities designed to acquire information concerning the personal circumstances of another individual or lends assistance not solely of an incidental nature to such activities, shall likewise be sentenced for unlawful intelligence activities.

For any such action to constitute *conducting activities* means that it must involve some degree of planning and organisation and comprise a series of actions that are of such a nature and close enough in time to be considered as a part of a larger scheme. Isolated actions are not regarded as criminal offences. However, the intention of gathering information of a specific nature constitutes sufficient grounds for the activities to be considered a criminal offence. This means that the mere existence of an organisation designed for that purpose, even if no information has yet been gathered by it, is sufficient for it to be deemed that such activities are being conducted.

The activities must also be conducted *secretly or by fraudulent means* in order to constitute a criminal offence. Secretly can mean that special caution is exercised when conducting the activities, such as communication at night at specially designated meeting places, through public telephone booths or via prepaid mobile phones. However, even when information is communicated in the normal fashion, unlawful intelligence activities can be the case if it is apparent that those who were conducting the activities presumed that the information was confidential and that what they were doing was illegal. Keeping secret the fact that one is conducting such activities as those described in the regulation can, in certain circumstances, be considered fraudulent.

The activities must involve obtaining information *concerning the personal circumstances of another individual*. Neither the wording of the provision nor the preparatory documents to the code explains in any further detail what is meant by this phrase but it can be assumed to include much of the information that can be linked to specific individuals. The purpose of creating this regulation was to penalize certain political intelligence activities targeting refugees and Swedish citizens and aiming to register e.g. their political views or racial backgrounds.

Personal Data Act

The Personal Data Act (1998:204), shall protect people from infringements upon their personal integrity caused by a processing of their personal data. It is a criminal offence to “intentionally or by gross carelessness” neglect to e.g. report partially or completely automated processing of personal data to the supervisory authority. The penalty is a fine or imprisonment of up to two years, depending on the severity of the crime (Section 49).

Breach of professional confidentiality

Breach of professional confidentiality is when a person discloses information which he is duty-bound by law or other statutory instrument or by order or provision issued under a law or statutory instrument to keep secret. The punishment is a fine or imprisonment for a maximum of one year. In petty cases, punishment shall not be imposed (Chapter 20, Section 3 of the Swedish Penal Code).

The Vienna Convention and international law

Under Article 31 of the Vienna Convention on Diplomatic Relations, a diplomatic agent shall enjoy immunity from the criminal jurisdiction of the receiving State. This means that no measures of execution may be taken by the courts in matters concerning criminal responsibility. A diplomatic agent is an ambassador or a member of the embassy’s (diplomatic mission’s) diplomatic staff.

Through the Vienna Convention, both diplomatic agents and certain premises were awarded inviolability, which means that they cannot be subject to criminal proceedings. The diplomatic mission’s premises and the diplomatic agents’ private residence shall be inviolable (Articles 22 and 30) and the archives and documents of the mission, wherever they may be, shall also be inviolable (Article 24). Diplomatic agents are inviolable and may not be arrested or detained (Article 29). At the same time, it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State, without prejudice to their privileges and immunities (Article 41).

It is generally recognised that under international law embassies have the right to take their own security measures in order to protect their embassy buildings and compounds, and other buildings or premises that are inviolable, e.g. the ambassador’s residence. These measures consist mainly of preventing unauthorised persons from entering the area or the building, carrying out checks of individuals who are found to be in the area and refusing entry to

people who have no authorization to be there. Such security measures may also be taken outside the embassy compound, if they are close enough to be considered as included in the protection of the embassy. The embassy's security personnel do not, however, have police powers. The receiving State has the duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage (Article 22, Paragraph 2).

The embassy has, for example, the task of ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State (Article 3 (d)). This is taken to also include the right to register information and to transfer this information to a database in the sending State. The embassy is also deemed to have the right to collect and register information relating to the security of the diplomatic mission. This does not only apply to information which can be linked to security within the embassy building but also to observations which are made in the immediate vicinity of the embassy. This may include suspected persons or vehicles. Diplomatic agents are not obliged to give evidence as witnesses (Article 31, Paragraph 2). This applies to both to the criminal investigation and during legal proceedings in a court of law. Under Section 3 of the Act which frees a foreign consul from the obligation to testify, etc. (1970:86), a person who is employed at a consulate in Sweden may refuse to give a statement concerning circumstances related to his performing the duties involved in his post. This exoneration from the obligation to testify regards both criminal investigations and trials and probably applies regardless of citizenship.

Chapter 23, Section 13 of the Swedish Code of Judicial Procedure

Under Chapter 23, Section 13 of the Swedish Code of Judicial Procedure, a person who refuses to make a statement concerning a matter of importance to the inquiry, may be questioned as a witness before the court.

The criminal investigation

Information from the US Embassy, etc.

A high-ranking diplomatic representative for the US Embassy in Stockholm was questioned for information. He has not abstained from his immunity from criminal responsibility or from his inviolability but has voluntarily presented himself for an interview. The following information emerged from that interview.

The Surveillance Detection Program (SDP) was created as a consequence of the bombing of the US Embassies in Kenya and Tanzania in 1998, in which more than 200 people lost their lives. The US Embassy began to plan for a

launch of the programme in Sweden in October 1999 and operations began in April 2000. The purpose of the programme was to systematically observe places in the proximity of diplomatically protected buildings and individuals in order to detect suspicious activities directed towards them. Observations that necessitate investigation are reported to the local police or to the Swedish Security Service. Surveillance is performed by a Surveillance Detection Unit (SDU). The unit consists of 5-10 people. SDP is a defensive programme that carries out observations. Such observations can also be made of demonstrations in order to receive an “early warning”, should they come to constitute a threat to the security of the Embassy. Investigative work is not permitted. The observations made are recorded and are an inviolable part of the archives of the Embassy. This inviolability also applies to all written reports. Consequently, the observations made by the SDU are inviolable. The SDU runs its activities from premises located in the vicinity of the Embassy. These premises are inviolable since they are a part of the diplomatic territory. These premises are used as a meeting place, to write reports and as a place to store equipment.

The USA claims, on its part, that there was a meeting between the Embassy's security officer and Sweden's Diplomatic Protection Group in the year 2000 concerning the SDP and that both parties accepted the working methods of the SDU. During the years 2002 and 2003, according to the USA, “live trainings” between the SDU and Sweden's Diplomatic Protection Group took place and in the year 2009 two Swedish Security Service employees visited the SDU premises together with the US Ambassador and received information there.

According to information from the USA, there is no documentation on this meeting and the training.

Information on the SDP, the SDU and on SIMAS has been on the Internet for a number of years. SIMAS is described as a worldwide web-based application which stores information on suspected activities and crimes that have been reported from US diplomatic missions. These reports usually include a description of the suspicious activity, the suspect, suspicious vehicle and any available identifying information (biometric information such as sex, race, height, etc.) and possibly photographs as well. If any other more detailed information such as name, citizenship, address, etc. is available, that is also recorded. Information on SIMAS can be found on the US Government's website.

The Foreign Affairs Manual (FAM) are regulations to be used internally by the US Foreign Service. Volume 12, Section 322 specifies that launching the SDP requires the approval of the government of the receiving state.

Information from Swedish authorities

I submitted a requisition to the Stockholm County Police, the Swedish Security Service, the Ministry of Justice, the Ministry for Foreign Affairs and the Swedish Armed Forces for copies of any annotations recorded in registers, including restricted ones, as well as of documents and the minutes of meetings (on paper or electronically) which can be associated in any way with the SDP or the SDU. This requisition applied to the period 1 October 1999 to the date of the requisition, which was 24 November 2010. Hereunder follows the information that emerged from this and is of relevance to the investigation.

The Stockholm County Police have no documents that can be associated with the aforementioned security activities. Certain documents, e.g. notes that patrolling officers make, are not registered or in any other way made searchable. However, during a witness interview with a representative for the Embassy Group, it emerged that in 2007 the Embassy Group, via the Swedish Foreign Affairs Ministry, sent a general request to every embassy for information on which security-enhancing measures they had taken. Neither the SDP nor the SDU was mentioned in that request. According to that witness, the US Embassy did not reply to the questions posed in the request.

The Swedish Security Service reported that there was no official notification or other declaration that the US Embassy had a program called SDP or a unit called SDU. However, throughout the years a number of reports concerning various incidents have come in from the Stockholm County Police. There have also been direct contacts between the Swedish Security Service and the Embassy concerning security matters, e.g. bomb threats. In a document received in 2005, the expression “SD specialist” was stated twice. On one occasion, in 2006, another European country asked the Swedish Security Service if the US Embassy in Stockholm had a “surveillance detection program”. According to witness statements taken from employees of the Swedish Security Service who answered this question in 2006, the Swedish Security Service had no knowledge of the SDP but they had been informed by Sweden’s Diplomatic Protection Group that there was a “surveillance team” which informed the police about its observations. In October 2009 the recently appointed US Ambassador, together with two close protection officers from the Swedish Security Service, visited premises in the vicinity of the US Embassy. These premises proved to be the aforementioned meeting place for the SDU. The Ambassador received information and the close protection officers met people who, according to information received, were part of the SDU/Stockholm. The close protection officers, who did not know about the existence of the SDU activities, wrote a memorandum about the visit. That memorandum prompted the Swedish Security Service to begin charting those activities. This charting has become a part of the investigation now underway.

The Swedish Ministry for Foreign Affairs informs us that in their records there is no official notification or other declaration on the part of the USA about the SDP or the SDU. However, an enquiry from a non-European country in 2002, asking whether Sweden is aware of any “Surveillance Detection” does exist. The administrative officer who handled this enquiry was questioned and said that the answer to the enquiry was that the Swedish Ministry for Foreign Affairs had no awareness of such surveillance.

The Swedish Ministry of Justice and the Swedish Armed Forces have informed us that they have no notification or other document indicating that the US Embassy accounts for or otherwise gives notice of the SDP or the SDU or such activities.

Visit in the SDU/Stockholm premises

I visited the SDU premises together with the investigators. The premises consisted of an approximately 30 square metre room containing some desks and computers and a storage cupboard. According to representatives of the SDU and the Embassy, these premises are used as a place to meet before a shift, for briefing and for storage of equipment and clothing. The equipment shown is deemed to be that typically used for surveillance, for example, heavy-duty clothing, binoculars and cameras.

The premises obtained diplomatic status in September 2010. The written documents that the US Embassy submitted to the Swedish Ministry for Foreign Affairs in order to have those premises approved for diplomatic immunity, do not indicate that the premises would be used for the SDU or for similar activities.

Interviews with individuals employed by the Stockholm County Police and by the Swedish Security Service concerning the SDP/SDU and Embassy contacts

Interviews were held with a number of individuals who are or were employed by the Stockholm County Police or by the Swedish Security Service. Individuals in both head and other roles were interviewed. The results of these interviews are summarized below.

Protection of foreign states' diplomatic missions in accordance with the Vienna Convention is shared so that Sweden's Diplomatic Protection Group takes responsibility for protection of places and buildings while the Swedish Security Service is responsible for the protection of diplomats. There is therefore well-established cooperation between these two policing organisations. Contacts between them and the US Embassy are frequent and have functioned well throughout the years. When incidents, suspects or vehicles in the vicinity of the Embassy are reported to the police, the matter is investigated. Annotations are

made or memoranda are written and information is reported back to the Embassy as deemed necessary (e.g. that nothing out of the ordinary has occurred). The Swedish Public Access to Information and Secrecy Act governs what information may be shared. Regular meetings concerning security arrangements take place, especially in association with relatively important events. Threat assessments are made in specific cases and also on a more general basis.

Those interviewed have not heard of the SDU or the SDP or anything similar before 2010, with three exceptions. Two of these exceptions regard the aforementioned close protection officers who visited the SDU premises and the question in 2006 to the Swedish Security Service from another European country. The third exception concerns the previous head of the Diplomatic Protection Group, who, during the course of the investigation, told about the following incident. In the summer of 2003 he was contacted by an individual he knew who was associated with the Embassy and he was asked to go to a place located in the vicinity of the Embassy. At this place, he was informed about the security programme for the US embassies, which had been put in place as a result of terrorist attacks in Africa. The abbreviation "SDT" was mentioned. The programme involved "strict observation" and the objects to be monitored were the embassy and the residence. He perceived the activities as harmless and as not in any way to go against Swedish legislation. He presumes that he reported his observations and his assessment of the incident to the Swedish Security Service.

Interviews with employees of the SDU

SDU employees were called in for interviews. All of those called in turned up and said that they work in the SDU or did so previously. They also stated that they cannot answer any questions on the activities of the SDU since they are bound by professional confidentiality. None of them have been employed by law enforcement agencies or by the armed forces. Some of them have stated that they got their jobs as a result of replying to a job advertisement for security specialists, which the Embassy had posted.

The US Embassy in Stockholm has explained, through its legal counsel, that a waiver of professional confidentiality should not be expected at this point in time. The USA claims that those observations made by SDU employees that were reported to SIMAS are to be considered as part of the Embassy's archives, which are inviolable under the Vienna Convention.

It is a matter of judgement whether the SDU employees can be considered as witnesses or as suspects in the criminal investigation. I have considered requesting the court to question them as witnesses so that their right to exercise professional confidentiality can be examined and to assess whether Section 3

of the Act which frees a foreign consul from the obligation to testify, etc. is applicable. If the court should find that they are to be considered witnesses and that they may neither exercise professional confidentiality nor exercise Section 3 of the aforementioned Act, they would have to take the oath, tell about the SDU activities, and have criminal responsibility. The court is, however, obligated to inform them, *before* their questioning as witnesses, of their right to decline to testify concerning a circumstance that reveals that they have committed a criminal act (Chapter 36, Section 6 of the Swedish Code of Judicial Procedure). I presume that they would exercise their right to silence whether or not they thought that they had done something illegal.

I have chosen not to petition the court in accordance with Chapter 23, Section 13 of the Swedish Code of Judicial Procedure.

Other information

All interviews were carried out in order to obtain information. None of the individuals interviewed has been given notice that they are under suspicion. During the investigation, there was also nothing to indicate that anyone has been or felt violated or observed by the SDU employees.

Assessment

Illegal intelligence activities

I deem it to be clear that the USA did not follow its own regulations (FAM, Volume 12, Section 322) that the SDP requires approval and support of the government of the receiving country. No information has been given to the appropriate authorities about the programme and the activities. Neither is there any statement from the USA that the Swedish government has been informed about and approved the programme. However, the USA (spokesperson Ryan Koch on Swedish television on 8 November 2010) claims that the “local authorities” were contacted and informed already at the beginning.

The question of whether the USA can be considered to have kept the SDP and the SDU secret would have penal relevance only if it can be proved that the activities, regardless of what they were called, that were actually carried out or were intended to be carried out were of the type punishable under Chapter 19, Section 10, Paragraph 2 of the Penal Code.

The first consideration is to what extent protective measures can be considered permitted under existing laws and conventions.

No special permission is required in order to establish a security unit at the Embassy. Such an organisation may carry out and make annotations of observations and take photographs for the purpose of protecting the Embassy and its staff. The Embassy's security personnel are permitted to have premises located outside the Embassy compound. Although the activities of the security personnel must be limited to the Embassy compound and its immediate vicinity, certain exceptions to this rule may be considered. If, for example, a demonstration that is to end near the Embassy has its starting point in another part of the city, the Embassy's security personnel are permitted to observe the demonstration already at its starting point in order to better evaluate its effect on security. Security personnel "shadowing" a suspect for a short distance within the vicinity of the Embassy compound in order to find out what this person is intending to do is something that I do not consider to be forbidden either.

Which sort of *activity* can then be considered a punishable offence under the provisions in the Penal Code concerning unlawful intelligence activities? Biometric information collected or photographs taken together with observations (e.g. of participation in a demonstration) which can be linked to a certain individual, can be considered as *information concerning the personal circumstances of another individual*. Operations which completely or partially consist of systematically gathering and recording such information can therefore be considered as unlawful intelligence activities. Systematically photographing individuals who are passing by the Embassy and, at the same time, collecting information which would make an identification of these individuals possible, e.g. registration numbers of the vehicles they are travelling in, can also be considered as unlawful intelligence activities.

During the years investigated, 2000-2011, the Embassy's security personnel have reported a number of incidents and posed a number of questions to both the Stockholm City Police and to the Swedish Security Service. From these encounters there is nothing which indicates that unlawful intelligence activities have been going on. On the contrary, the content of the annotations and reports which were inspected are of the kind to be expected of security operations, e.g. suspicious behaviour, suspicious vehicles and bomb threats. No individual has come forward and described actions which could indicate that unlawful activities have been carried out against him or her. The actual purpose of the operations does not appear to be the politically motivated espionage envisaged by the legislators as an example of unlawful intelligence activities.

Information registered in SIMAS however, can be such information on personal circumstances referred to in Penal Code provisions concerning unlawful intelligence activities. I think this is evident from the information about the database which can be found on the US Government website. If the intention of launching the SDP in Sweden was for the SDU to report

information on personal circumstances to SIMAS or to some similar register, already the existence of an organization like the SDU could be sufficient to constitute a punishable offence under Chapter 19, Section 10, Paragraph 2 of the Penal Code. In order to assess both the purpose of the SDU and what observations the SDU reported, it would have been necessary to interview SDU employees without restrictions and to gain access to the Embassy's records, inclusive SIMAS, in order to check the information received during these interviews against the records. Vienna Convention regulations do not allow access to any of this information. Consequently, it cannot be proven that unlawful intelligence activities have taken place and the investigation will be discontinued.

Crimes against the Personal Data Act

The information obtained from monitoring and security work may be registered and processed in a database at the Embassy or in the sending state under international law and the Vienna Convention. No permission from Swedish authorities is necessary. I do not believe that I should attempt to determine whether these regulations permit or were intended to permit registration of personal information referred to in the Personal Data Act or of personal circumstances referred to in the provisions on unlawful intelligence activities, considering that the sending state shall, in principle, follow the laws of the receiving state. As is apparent from above, the Embassy has not handed over any information from its records. What these records, including SIMAS, actually contain can therefore not be investigated. The investigation will therefore be discontinued.

Breach of professional confidentiality

There is nothing to indicate that breach of professional confidentiality was committed. Since there is no reason to believe that such a crime was committed, the investigation will be discontinued.

Tomas Lindstrand