

ВЛИЯНИЕ НА СОЦИАЛНИТЕ МРЕЖИ ВЪРХУ НАЦИОНАЛНАТА СИГУРНОСТ

Д-р Валентина Хорозова

Академия на Министерството на вътрешните работи

Резюме: В настоящата разработка е представено как функционирането на съвременното общество в национален и глобален аспект придоби предречения от много автори „информационен характер“ и засегна дълбоко личния живот, политика, дипломация, сигурност, социални процеси, бизнес. Застъпена е тезата как нови глобални тенденции доказват появата и възможностите на новия колективен субект на международната сцена – социалните мрежи. С оглед актуалността на проблема в настоящата статия ще дадем определения и характеристики на социалните мрежи, като обърнем повече внимание на влиянието им върху сигурността и обществения ред.

Ключови думи: сигурност, социални мрежи, интернет.

INFLUENCE OF SOCIAL NETWORKS ON NATIONAL SECURITY

Head Assistant Professor Valentina Horozova,
Academy of the Ministry of Interior

Abstract: This paper presents how the functioning of modern society in national and global aspect has acquired predictions by many authors "informational nature" and deeply affected privacy, politics, diplomacy, security, social processes, business. The thesis is how new global trends prove the emergence and capabilities of the new collective subject on the international stage - social networks. In view of the topicality of the problem in this article we will

give definitions and characteristics of social networks, paying more attention to their impact on security and public order.

Key words: security, social networks, Internet.

УВОД

През 2020 г., след протестите против правителството в Република България и безпрецедентната атака на Капитолия в началото на 2021 г. никой вече не се съмнява във възможностите на новия колективен субект – социалните мрежи. Новите форми на комуникация все по-осезаемо заменят информационните контакти от лични (непосредствени) към опосредствани с техническите средства. Това стана възможно благодарение на интернет и на базираните в него мрежи. Мнението за тях е противоречиво, но когато 2020 г. бе блокирана от Ковид - 19 те се оказаха животоспасяващи и за най-отдалечените и изостанали краища. Дори контактите между лекари и пациенти минаваха през тях. Така функционирането на съвременното общество в национален и глобален аспект придоби предречения от много автори „информационен характер“, засегна дълбоко личния живот, политика, дипломация, сигурност, социални процеси, бизнес. С оглед актуалността на проблема в настоящата статия ще дадем определения и характеристики на социалните мрежи, като обърнем повече внимание на влиянието им върху сигурността и обществения ред.

Социалните мрежи като колективен феномен и проблем за управлението

Социалните мрежи, базирани в интернет станаха предмет на задълбочени изследвания. Руски автори оформиха мнението, че под социална мрежа се разбира социална структура от неопределен брой агенти (субекти – индивидуални или колективни, например, индивиди, семейства,

групи, организации), организирани по интереси, чрез които се създават кратки или постоянни връзки между хората като, например познанства, приятелство, сътрудничество, комуникация, бизнес. Тази внасяща спокойствие дефиниция бързо бе опровергана от Марио Масдеа. Според него социалните медии трябва да се разглежда като мощно оръжие. Всички държави и организации като НАТО вече използват комуникациите за постигане на определени цели. Джон Аркуила и Дейвид Ронфелд дефинираха ново понятие - мрежовата война. Според тях тя представлява „нова форма на конфликт, в който главните герои - вариращи от терористични и престъпни групи до войнстващи социални активисти - използват мрежовата форма на организация, доктрина, стратегия и технология, съответни на информационната епоха.“ Оказа се, че мрежова война (плод на Индустрия 4.0) е много по-напред от осмислянето на теорията и последиците от нея. Освен информационните технологии, бързия достъп до бази данни и огромен брой потенциални потребители, епохата роди авангардна престъпност, нови поколения социални революционери, радикални активисти, анархисти, нихилисти, идеолози, терористи и пр., които на транснационалното равнище създават новите структури на "глобалното гражданско общество." Виждаме първия проблем – държавата (структурите за НС) не може да се намеси ефективно. Най-опасна се оказва симбиозата между радикални идеи и лидери + масови социални недоволства по всякакъв повод. Спонтанната или целенасочената организация на тези феномени от една страна и противодействието чрез органите за сигурност според теоретиците има характера на "мрежова война", която може да има ясни лидери или да протича хаотично, т.е. неконтролирано. Някои считат, че това ще бъде „общественият конфликт през 21-ви век.“ Джоел Гаро предполага, че мрежова война се печели от страната с по-висш интелект и

технологии. Т.е. от този, който организира бързо противодействие на противниковата социална мрежа с контра-мрежи, хакери и бързо ориентирани се управленци. Но въпросът за НС е кой ще победи – тези, които управляват държавата или тези, които искат да я разрушат с използването на маси от недоволни хора, които с телефоните си ще излязат на улицата?

Очевидно е, че трябва да приемем изводите на авторите, които казват, че НС изградена от гарантирани затворени системи, няма да бъде неефективна, защото ще живее за себе си и общественият океан ще помете установения конституционен ред. Видяхме го при старта на Арабските революции след 2010 г., но мащабите изненадаха Европа – миграционните потоци се прехвърлиха чак в Швеция със своите радикални идеи, религиозни особености и лични проблеми.

Проф. Цветан Семерджиев ("Войната на мрежите", "Сигурност и защита на информацията") разсъждава върху предимствата на йерархичната и мрежовата армейски и институционални архитектури, и плоските престъпни и терористични клетки, които чрез общодостъпните информационни технологии елиминират йерархичните звена, които бавят и изкривяват информацията и управленските цели. Първите струват много пари, вторите се самоизграждат, затихват или ескалират с милиони привърженици.

Проблеми при правната регламентация на поведението в социалните мрежи.

Навлизането на интернет технологиите във всички сфери на обществения живот предизвикват достигането на огромен поток информация от всички точки на света до всички потребители на глобалната

мрежа Грета Дерменджиева¹ отбелязва, че новоформираното глобално информационно общество се отличава с т.нар. дигитализация на информацията, чрез която става възможно и пренасяне на сложни съчетания на различни видове данни - текст, звук, статични и динамични изображения (мултимедия). На следващо място се забелязва експоненциално нарастване на данни и тяхното разпространение; достъп до информация във всяка точка от света; безжични услуги с глобално покритие; интелигентни мрежи с интерактивни услуги; информационни услуги като нови форми на дейност.² Традиционните средства за масова информация отстъпиха място на социалните мрежи, които не само станаха източник на информация, но и източник на директно споделяне и направляване на общественото мнение. Т.е. гражданите от потребители на информация се превърнаха в създатели на информация и субекти на социално-политическо въздействие. Логична последица от всички тези промени са сериозни социални изменения и ефекти и то в глобален аспект. Скот Лаш отстоява тезата, че съвременната социална класа и социалното неравенство вече зависят от достъпа до информация, а не от начина на производство.³

Без участието на държавата и институциите бе създадено виртуално общество, в което неформални групи от различен характер, на много места предизвикаха дестабилизация на обществото във всички аспекти на социалния живот. Това бе плод на новия вид комуникация и новата класа, където намериха почва освободено поведение, вербална агресия, недружелюбно поведение, рядко проявление на позитивни междуличностни взаимоотношения, по-безличностна комуникация, която води до

¹ Дерменджиева, Г. Увод в компютърно-опосредстваната комуникация. Университетско издателство „Св. Климент Охридски“, София, 2001 г

² Дерменджиева, Г. Цит. съч.

³ Лаш, С. Критика на информацията. София, ИК „Кота“, 2004 г

деперсонализиращ ефект, а като резултат - по-висока степен на промяна на решението, намалена адаптивност, труден консенсус. Всичко това несъмнено може да доведе до разклащане на съществуващото статукво, срив на йерархията и подмяна на досегашните роли в дадена група, организация и в обществото.⁴ Този нов вид дестабилизиращи процеси не биха могли да се повлияят в необходимата степен от досегашните методи и средства за опазване на сигурността, обществения ред и обезпечаване на нормалното функциониране на институционалния ред в национален и глобален аспект. Очевидно е, че глобалната интеграция на информационното пространство постави институциите за сигурност и обществен ред в „шок от бъдещето“ – никой не знаеше, не можеше да предположи и да контролира изхода от социалната активност. На този фон законодателството в световен мащаб започна да търси законови и практически форми на контрол както на интернет мрежата, така и на социалните медии в нея. Успехи не бяха постигнати още в началото, когато САЩ опита да ограничи интернет пиратството и да гарантира авторските права (Stop Online Piracy Act (SOPA) и Protect IP Act (PIPA). Не успя и Търговското споразумение за борба с фалшифицирането АСТА - Anti-Counterfeiting Trade Agreement, насочено против контрабандата и търговското разпространение на фалшиви стоки в ЕС и САЩ. Противдействието започна още в американския Сенат и Европейския парламент. На този фон многохилядни протести се обявиха против опитите за следене на интернет потребителите, че то може да се използва за тотално следене в глобалната мрежа и ограничаване на основни човешки права.

Така стигнахме до 2021 г., когато „Социалната мрежа Туитър съобщи, че след размириците на Капитолия в началото на месец януари 2021

⁴ Дерменджиева, Г. Цит. съч

година е преустановила достъпа до над 70 000 профила, свързани с крайнодясната конспиративна теория "КюАнон" (QAnon). Шокиращото беше, че бе отнет достъпа на президента на САЩ Доналд Тръмп. Освен Туитър, други две от най-популярните платформи – Фейсбук и Инстаграм също свалиха профилите на американския президент. Тези безпрецедентни действия бяха последвани от технологичните гиганти – Епъл, Гугъл и Амазон, които не след дълго спряха да работят с популярната сред привържениците на президента социална мрежа Парлър. С това свое действие, те буквално замразиха дейността й.⁵

Безпрецедентното отнемане на достъпа на президента на една от най-свободните държави в света до редица социални мрежи бе посрещнато с противоречиви мнения. Важно следствие от събитията без аналог в историята на човечеството е факта, че сред полярните мнения по този въпрос, на преден план се стигна до изводът, че правната регламентация на функционирането на социалните мрежи не работи и правителствата и корпорациите ще трябва да вземат силови решения. Германският канцлер Ангела Меркел, чрез свой говорител заяви, че "Правото на свобода на мнението е фундаментално право. Всяко ограничаване на това право може да става по силата на закон, а не от частна компания". Според еврокомисаря за вътрешния пазар и услуги Тиери Бретон е "смущаващо" как с едно свое решение, неподлежащо на проверка и коментар, изпълнителният директор на технологична компания може да вземе "високоговорителя" от президента на САЩ. Според него това е пример за сериозните слабости на съвременното общество по отношение на дигиталното пространство.⁶

⁵ <https://www.svobodnaevropa.bg/a/31043417.html> - посетен на 18.01.2021

⁶ Пак там

Основният извод от анализа е ясен – социалните мрежи могат да имат позитивни или дестабилизиращи ефекти върху националната сигурност. Правната регулация върви след събитията и среща съпротива от обществеността. Ние считаме, че социалните мрежи, ориентирани към услуги и бизнес по-скоро трябва да бъдат пространства на свободно лично и корпоративно предприемачество. Но и там контролът е необходим – разпространението на стоки с възможна двойна употреба, лекарства, измами и контрабанда придобиват широки размери.

Влияние на социалните мрежи върху средата за сигурност и обществен ред

Компютърните социални мрежи стартират на 2 октомври 1971 г. и са създадени от хората, които за пръв път ползват електронна поща. Не е случайно, че това са американски военносслужещи, използващи мрежата ARPANET. Постепенно новите форми на комуникация започват да изместват информационните контакти от лични (директно общуване) към опосредствани с техническите средства и възможности на интернет и на базираните в него социални мрежи. Днес имаме тотално променен начин на живот и качествено нови възможности за интензивни контакти в реално време. Феноменалното е, че те могат да се насочват от определени цели, да създават групи по интереси и да селектират различни пластове на обществения живот. Ако приемем, че средата за сигурност има няколко нива (локално, регионално, национално и глобално) така трябва да бъдат класифицирани и социалните мрежи. Въздействието върху тях може да бъде политическо, икономическо, социално, технологично, природоклиматично, културно, правно, екологично. На практика обаче всичко тези фактори действат едновременно и трудно предсказуемо (целенасочено, хибридно). Поради това според нас въздействието върху социалните мрежи крие

рискове от разрушителни процеси. Естествено, конкурентите и противниците могат да ги предизвикат лесно или да използват вече функциониращи общности с провокативни съобщения, слухове, провокатори и манипулации. Дори ако са разпространени в сферата на услугите, транспорта, здравеопазването и други, те бързо прерастват в проблем за националната сигурност. Това поставя въпроса как да бъде организиран контролът върху социалните медии, какъв модел на контрол е допустим и законосъобразен, как да се регулират отношенията между социалните медии, гражданското общество и институциите за сигурност и обществен ред. Много автори сочат, че руският модел е много ефективен чрез активното инфилтриране на подготвени лица във форумите за формиране и насочване на общественото мнение. Китайският и арабските модели включват директни забрани на определени социални мрежи, които се заменят с държавно управлявани. В САЩ бе създадена система тотално наблюдение на социалните мрежи и протичащата през тях информация. Тя обхваща дори териториите на съюзниците, което предизвика бурни дебати в ЕС. През 2013 година избухна скандал, след като в медиите изчете информация, че комуникациите на германския канцлер А. Меркел вероятно са били наблюдавани от Вашингтон. Следователно, ако в социалните мрежи, ориентирани към услуги и бизнес контролът трябва да е минимален, то в сферата за националната сигурност той трябва да е детайлно регламентиран. Той трябва да обхваща лични данни, бази данни на институциите и всички обекти визирани със защита на класифицирана информация. Според Николай Слатински конфликтът между йерархичния характер на институциите в системите за сигурност и мрежовия характер на свободно формиращите се социални мрежи ще бъде трудно разрешим. Той казва, че колкото в по-голяма криза е една държава, колкото по-нестабилна е тя,

толкова повече проблеми стават проблеми на сигурността. Република България е на периферията на ЕС, подложена е на силни въздействия и според нас е държава от тази категория.

В актуализираната Стратегията за национална сигурност на Република България от 2018 г. (Приета с Решение на НС от 14.03.2018 г., обн., ДВ, бр. 26 от 23.03.2018 г)⁷ тази проблематика се визира в раздел трети и намира място сред актуалните рискове и заплахи на средата за сигурност. Развитието на информационните и комуникационните технологии предопределя все по-голямото значение на киберпространството за гражданите, публичната власт и деловите среди. От ключово значение за националната сигурност са изведени правилното функциониране и устойчивост на информационните системи; противодействието на киберпрестъпленията; адекватна борба и справяне с хибридните действия и хибридните способности за водене на война и свързаните с тях последици; ограничаване на възможностите киберпространството да се използва от организирани престъпни групи или от терористични групировки.⁸

Ще дадем пример с една типична с мрежа, която промени средата за сигурност в световен мащаб в условията на глобалната виртуална реалност - WikiLeaks. Тя бе създадена като социална мрежа с широко участие на субекти и възможност за анонимно редактиране на статии. На сайта бяха публикувани стотици хиляди секретни документи от различни източници, включително анонимни, които разобличават корпоративната и правителствената корупция в различни държави. WikiLeaks използва сървъри в държави, чието законодателство осигурява по-голяма автономност. Сътрудниците на сайта използват кодирани комуникации, за

⁷ Стратегията за национална сигурност на Република България от 2018 г.

⁸ Пак там.

да не могат да бъдат проследени. Журналистите на "WikiLeaks " използват криптирана връзка, за да получават строго секретните документи. Затова те рядко узнават самоличността на своите източници и унищожават информацията, свързана с тях. За сайта работят на доброволни начала хиляди хора, сред които журналисти, програмисти и правозащитници. Така за броени месеци WikiLeaks публикува над един милион секретни и строго секретни документи с експлозивно съдържание. Те нанесоха непоправими щети на НС на САЩ и компрометираха отношенията със съюзниците им.

ЗАКЛЮЧЕНИЕ

Цялостно погледнато, опитите да се отдели личната, гражданската, националната и съюзническата (в ЕС и НАТО) сигурност в социалните мрежи не постига резултати. Проблемите на държавата бързо стават проблеми на отделния гражданин и обратно. И всичко това се оказва в полето на сигурността. Пандемията Ковит-19 показва, че първоначално хората, лекарите и фармацията бяха оставени на свободно договаряне, което създаде общества от недоволни и потенциал от заплахи. Наложих се държавата да поеме управлението на процеса, но и до сега широки обществени кръгове са недоволни на фона на слуховете относно ваксините, последиците и приоритетите.

Прогнозата е, че социалните мрежи от обикновена комуникационна среда все по-бързо се превръщат в силен и непредсказуем играч на социално-политическата сцена и стават генератор на политически революционни промени – демократични и антидемократични. Интернет базираните социални медии са ново пространство, родено от Индустрия 4.0 наречено „дигитална гражданска инфраструктура“. При неадекватен контрол (правен, технологичен, организационен, институционален) те се превръщат в елемент от т.нар. “рисково общество” – социално-

политическото управление се залива от информация и субективни нагласи, на които институциите не могат да реагират бързо и адекватно. Намесата на анонимни зловредни актьори в това поле вече е доказана практика и заплахата вече може да се дефинира като целенасочена. Това превръща социалните мрежи в социално-политически океан, където хищниците могат да се превръщат в основни модератори.

Въпросът за влиянието на социалните мрежи и социалните медии базирани в интернет върху процесите в сигурността, обществения ред и отбраната поражда две тенденции - рискове и заплахи за националната сигурност или ползи за националната сигурност. Според нас решаваща роля за успеха в новата среда има контролът от страна на държавата. Това среща яростна съпротива от правозащитници и цели социални групи особено в ЕС. Въпреки това автори като Вл. Иванов още през 2005 година изразяват становище, че трябва да се гради единна централизирана и йерархична европейска система за гранична охрана от хомеостатичен тип, която да идентифицира и допуска в общностното пространство само позитивни процеси. Това означава граничен, миграционен, митнически, финансов, здравен, отбранителен и виртуален контрол.⁹

Според нас, социалните мрежи ще продължат да живеят в хаоса на глобализацията и най-засегнати ще бъдат развитите общества. Престъпните групировки ще бъдат улеснени от неефективния йерархичен модел на институциите. Те се възползват от плоския мрежов модел, за който не са необходими ресурси и асиметричните заплахи могат да се генерират по всеки повод. Това поставя системата за НС пред сериозни законодателни, организационни и кадрови промени

⁹ Иванов, Вл., Охраната на държавните граници и новият световен ред. С., 2005 г., с. 161 – 170.

Използвана литература:

1. Стратегия за Национална сигурност на Република България. Приета с Решение от 08.03.2011 г. на Народното събрание, актуализирана с Решение на НС от 14.03.2018 г., обн., ДВ, бр. 26 от 23.03.2018 г
2. **Дерменджиева, Г.** Увод в компютърно-опосредстваната комуникация. С., Университетско издателство „Св. Климент Охридски“, 2001 г
3. **Иванов, В.** Охраната на държавните граници и новият световен ред. София, 2005, ISBN 954-509-324-2, с 161-170
4. **Лаш, С.** Критика на информацията. София, ИК „Кота“, 2004 г.
5. **Семерджиев, Цв.** Войната на мрежите. С., Софттрейд, 2002 г.
6. **Семерджиев, Цв.** Сигурност и защита на информацията. С., издателство „Класика и стил“, 2007 г.
7. **Слатински, Н.** Конфликти и сигурност: йерархични vs мрежови структури, <http://nslatinski.org>
8. **Раянова, Кр.** Институционализиране на тероризма като фактор за социално-политическо унищожаване в контекста на развитието на глобалните социално-политически процеси, Русенски университет "Ангел Кънчев, 2016, Научна конференция, ISSN 1311-3321; ст. 136-148
9. **Раянова, Кр.** Същност на концепцията за национална сигурност (Essence of the concept of national security), Русенски университет "Ангел Кънчев, - 2018, volume 57, book 7, ISSN 2603-4123 (online) стр. 163 - 168
10. <https://www.svobodnaevropa.bg/a/31043417>.