Дмитрий Нурумов
Главный правовой советник
Центра Исследования Правовой Политики (LPRC)

КОММЕНТАРИЙ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ COVID-19

В соответствии с Законом «О чрезвычайном положении» РК, меры, применяемые в условиях чрезвычайного положения, и ограничения прав и свобод физических лиц должны осуществляться в пределах, которые вызваны обстоятельствами, послужившими основанием введения чрезвычайного положения. Также в соответствии с этим Законом меры и ограничения, применяемые в условиях чрезвычайного положения, не должны противоречить международным договорам в области прав человека, ратифицированным Казахстаном. Чрезвычайное положение не означает, что можно пренебречь действующим законодательством по правам человека и международными обязательствами, в том числе в области защиты персональных данных. Отступления возможны, но они должны быть законны, оправданы, пропорциональны и ограничены во времени.

30 марта в ходе онлайн брифинга заместитель акима г. Нур-Султана Малика Бектурова озвучила, что власти города намерены контролировать людей, находящихся на карантине при помощи мобильного приложения «Smart Astana». Однако, не совсем ясно каким образом будет работать данное приложение. По-видимому, приложение позволяет отслеживать тех, кто находится на домашнем карантине (через некий ситуационный центр). Со слов спикера, это приложение будет контролировать соблюдение этими лицами главного условия домашнего карантина – не покидать своего дома или квартиры.

На данный момент не известно будет ли приложение обязательно к использованию уже заболевшими лицами или, например, в отношении всех прилетевших из-за границы или же в отношении любых граждан, которые находятся в группе риска. Насколько это необходимо, когда уже объявлено о массовом всеобщем карантине в ряде городов Казахстана? Потенциально такие системы слежения можно распространить на любых жителей страны и контролировать соблюдение ими режима ЧП, и не только ЧП.

Кроме функции контроля геолокации лица, можно предположить, что будут логироватся, как минимум, мета-данные с телефона лица, который установил (или которого обязали установить такое приложение) и телефонов, которые будут находиться в определенном радиусе от телефона лица, который загрузил данную программу, причем в течение определенного времени (например, 30 дней). Это могут быть мета-данные real time или данные, логируемые с определённым временным лагом. Объём таких мета-данных и степень их индивидуализации может отличаться. Полученные мета-данные могут быть использоваться для выявления контактных лиц или рассылки потенциальным контактным лицам общих или персонифицированных сообщений (в том числе по принципу светофора, где каждый цвет будет

обозначать степень риска и/или побуждать лицо к действию, например, сообщить о своем местонахождении, предоставить свои анкетные данные или скан удостоверения личности, пройти обязательное тестирование, передать показания температуры своего тела и т.д.).

Ведется ли в данный момент анализ мета-данных по геолокации телефонов в Казахстане и как используются эти данные остается отрытым, так как такой сбор больших агрегированных данных может происходить и без всяких приложений. Причем, если требуется, деанизимация мета-данных, то она может быть осуществлена достаточно быстро в рамках имеющихся полномочий соответствующих государственных органов.

На данный момент четкой правовой базы для использования таких технологий, в том числе подобных приложению «Smart Astana», в Казахстане нет. Может ли Министерство здравоохранения своим постановлением или Главный санитарный врач своим приказом обязать использовать такие приложения и, более широко, пусть и временно, на период ЧП, институционализировать систему слежения через анализ геолокации и данных по перемещению физических лиц является спорным, так как речь идет о внедрении системы, которая получит доступ к персональным данным граждан, а также может ограничивать право на частную жизнь, право свободу передвижения и др. основные права. Конечно, полномочия врачей в том числе по карантину никто не собирается оспаривать. Вопрос здесь в том, что использование систем слежения на основе массовой геолокации имеет много побочных рисков, которые могут выходить за рамки рисков, связанных с обеспечением стандартных карантинных мероприятий.

Несмотря на то, что многие страны Юго-Восточной Азии, Израиль и ряд стран Европы применяют или изучают возможности использования подобных технологий в рамках ответа на COVID-19, например, для отслеживания контактных лиц или за передвижением граждан с целью оценки эффективности своих мер по недопущению скопления людей в тех или иных публичных пространствах, некоторый накопленный исторический опыт говорит о том, что сами по себе мета-данные по перемещению и геолокации могут и не оказывать решающее значение в борьбе с болезнями или их распространением. Вполне возможно, что подобные системы слежения сыграли определённую положительную роль в ряде стран сейчас – при пандемии COVID-19, но важно учитывать контекст и обстоятельства, в которых они были развернуты. Например, в той же Южной Корее большую роль (если не решающую) играло тестирование. Большую роль также сыграли ответственность граждан, социальное дистанцирование, готовность к подобным ситуациям, предыдущий опыт с sars и другими подобными вирусами. Кроме того, в Южной Корее одна из лучших медицинских систем в мире. Кроме того, возможно такой электронный мониторинг в домашних условиях как альтернатива помещения в обсервацию имеет смысл на более ранних этапах распространении вируса, а не в условиях уже случившегося массового карантина.

В любом случае, такие экстраординарные меры не должны развёртываться без оценки рисков и обеспечения эффективных гарантий. Чрезвычайные меры требуют особой чувствительности к возможным рискам. Например, не ясно на данный момент будут ли телекоммуникационные компании предоставлять доступ к первичным данным или же они будут проводить анализ данных на основе параметров, которые будут устанавливаться каким-то государственным ведомством. Однако, в любом случае, вопрос прозрачности подобных систем слежения и эффективности надзора за ними в наших условиях вызывает озабоченность, и тем более при чрезвычайном положении. Сами по себе такие системы слежения по геолокации телефона (симкарты) не дают стопроцентной гарантии что будут засечены все контакты. Лицо может

оставаться на «цифровом поводке», но никто не застрахован, что оно может контактировать с лицами, которые смогли специально или не нарочно «замести» свой цифровой след. Есть много способов обойти такие системы слежения и самими лицами в отношении которых принято решение об использовании такого приложения.

Кто несет ответственность если информация, которая была таким образом собрана и не оказалась достоверной? Что если конечный пользователь такой информации совершил определенные действия на основе этой информации? Что если такая информация стала публичной? В ряде стран, где такая система слежения уже использовалась не всегда было понятно почему, то или иное лицо получало сообщения на свой телефон и насколько они являлись достоверными. Не исключено, что в определенных случаях такая информация запутывала граждан с одной стороны, а с другой - создавала ложную иллюзию контроля у властей.

Цель любых ограничительных мер при ЧП должна быть максимально ясной, но это недостаточно. Любые такие меры, как и другие меры в подобной ситуации, должны применяться только на основе мнения специалистов в сфере здравоохранения и основываться на соответствующей доказательной базе. Достичь другими способами эту цель невозможно. Исторически, даже если чрезвычайные положения отменялись, многие временные меры приживались. Поэтому важно учитывать не только краткосрочные, но и долгосрочные последствия. В любом случае, персональные данные не должны использоваться для других целей и своевременно удаляться, а граждане должны иметь эффективные гарантии, что любые новые технологии, не приведут к необоснованному ограничению их прав, даже в экстраординарной ситуации борьбы с COVID-19.

9 апреля 2020